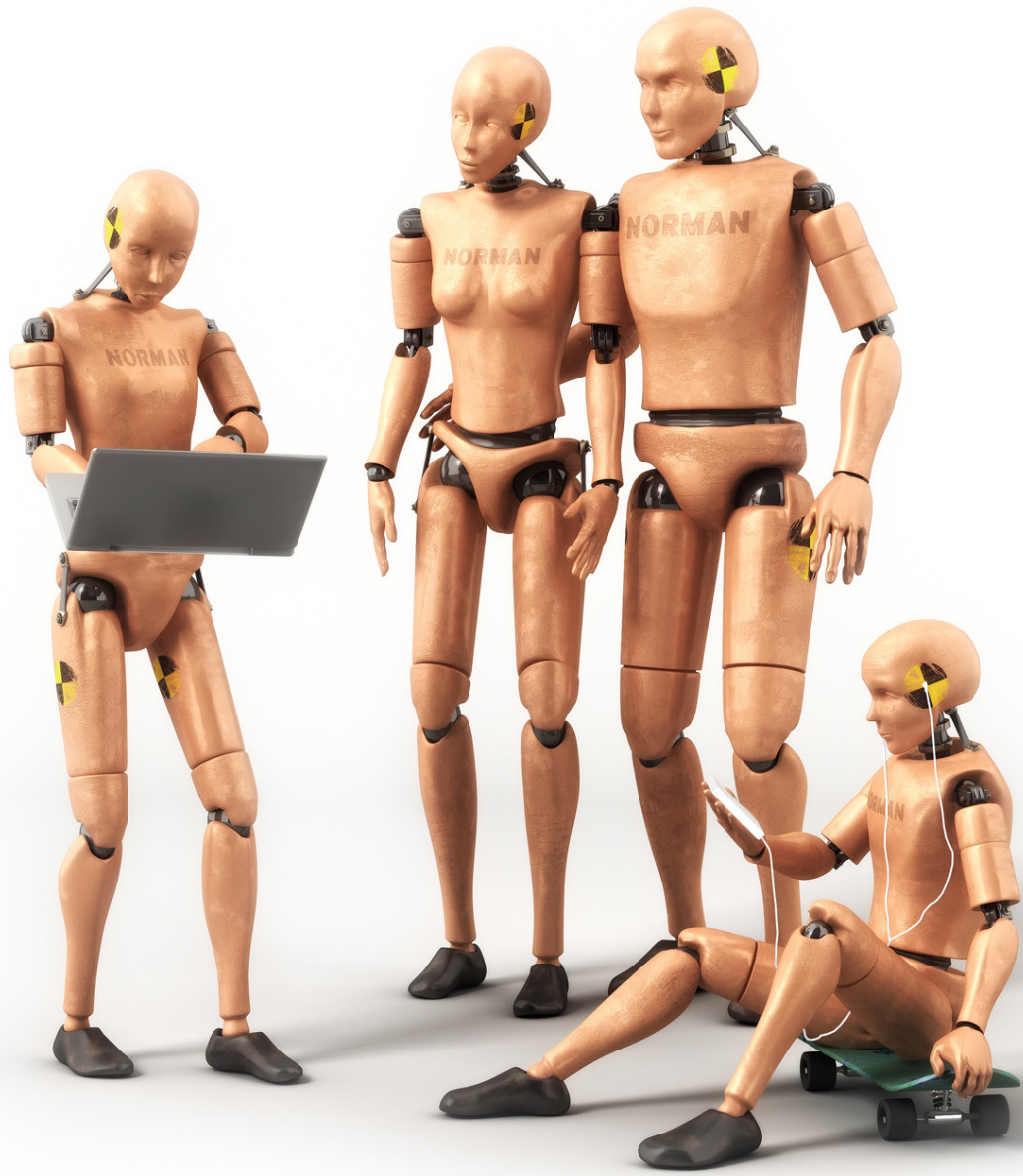
NORMAN

SecuritySuite

Guia do Usuário

versão 8.00



SAND BOX STATIS-TICS UPDATE UNREAD MAIL SECURED VIRUS SCAN DOCU-MENTS

- Antivirus
- Antispam
- Intrusion Guard
- Personal Firewall
- Parental Control
- Privacy Tools

NORMAN®

Garantia limitada

A Norman garante que o CD-ROM ou DVD e a documentação anexos não contêm falhas de produção. Se você relatar uma falha em 30 dias a partir da data da compra, a Norman substituirá o CD-ROM ou DVD e/ou a documentação sem custo algum. Deve-se incluir o comprovante da compra em qualquer solicitação.

Esta garantia limita-se à substituição do produto. A Norman não é responsável por nenhuma outra forma de perda ou dano resultante do uso do software ou documentação ou de erros ou deficiências em tais itens, incluindo, sem limitação, lucros cessantes.

Com respeito a defeitos ou falhas no CD-ROM, DVD ou na documentação, ou neste contrato de licenciamento, esta garantia substitui quaisquer outras, expressas ou implícitas, incluindo, sem limitação, as garantias implícitas de comerciabilidade e adequação para um fim específico.

Especificamente, e sem as limitações impostas pelo contrato de licenciamento com respeito a qualquer uso ou fim especial, a Norman, em nenhuma hipótese, será responsável por lucros cessantes ou outros danos comerciais, incluindo, sem limitação, danos incidentais ou imprevistos.

Esta garantia expira 30 dias após a compra.

As informações neste documento bem como a funcionalidade do software estão sujeitas a alteração sem prévio aviso. O software poderá ser utilizado em conformidade com os termos do contrato de licenciamento. O comprador poderá fazer uma cópia do software para fins de cópia de segurança. Nenhuma parte da presente documentação poderá ser reproduzida ou transmitida, qualquer que seja a forma ou meio, quer eletrônico ou mecânico, incluindo, sem limitação, fotocópia, gravação ou armazenagem de informações e sistemas de recuperação, para qualquer outro fim que não para uso pessoal do comprador, sem autorização explícita e por escrito da Norman.

O logotipo da Norman é marca comercial registrada da Norman ASA.

Os nomes dos produtos mencionados nesta documentação são marcas comerciais ou marcas comerciais registradas de seus respectivos proprietários. São mencionados apenas para fins de identificação.

A documentação e o software da Norman são

Copyright © 1990-2010 Norman ASA.

Todos os direitos reservados.

Revisado em março de 2010.

Apresentação 4
Requisitos do sistema 4
Sobre esta versão 4
Sobre este manual 4
Treinamento e Suporte Técnico 4
O que é o Conjunto de Segurança Norman? 5
Antivirus & Antispyware 5
Personal Firewall 6
Antispam 7
Parental Control 7
Privacy Tools 7
Intrusion Guard 8

Instalação 9
Recuperando o software 9
Chave de licença 10
Instalação 10
Assistentes 12
Assistente de Instalação 12

Guia de Introdução 13
Ícone da bandeja do aplicativo 13
Os ícones de aviso da bandeja 14
Abrir o aplicativo 15
Ícones de aviso do produto 15
Configurações do Security Suite 15

Página Principal 16
Atualizar todos os produtos 16
As atualizações automáticas estão ativadas (on)/desativadas (off) 16

Antivirus & Antispyware 17
Visualização principal 17
Quarentena 18
Manter arquivos em quarentena 18
Arquivos em quarentena 19
Editor de Tarefas 19
Criar uma tarefa 20
Programar verificações 21
Lista de exclusão 21
Configurações 22
Verificador automático 23
Verificador manual 25
Proteção da internet 26
Outros métodos de verificação 29

Personal Firewall 31
Visualização principal 31
Ferramentas de Perito 33
Editor de regras 33
Utilitário de registro em tempo real 36
Visualizador avançado de portas 37
Exportar regras do Personal Firewall 38
Importar regras do Personal Firewall 38
Configurações 39
Configurar o Personal Firewall 39
Configurações avançadas 39

Antispam 40
Visualização principal 40
Bloquear/Permitir 42
Adicionar/remover endereço de e-mail 42
Configurações 43
Configurar nível de rigor do filtro 43
Configurar controle de spam 43

Parental Control 44
Visualização principal 45
Configuração do usuário 46
Configurações padrão de perfil 47
Criar usuário 48
Visualizador do registro 50
Configurações 50

Ferramentas de Privacidade 51
Excluir um histórico de programa do usuário 51
Exclusão Segura 52

Intrusion Guard 53
Visualização principal 53
Configurações 53
Drivers e Memória 54
Processos 55
Rede 56

Instalar e atualizar 57
Visualização principal 57
Configurações 58
Selecionar o método de atualização 58
Configurações de proxy 59

Centro de Suporte 60
Visualização principal 60
Ajuda e resolução de problemas 60
Informação de contato 60
Reparo automático 61
Visualizador de Registro de Mensagens 61

Desinstalação do NSS 62

Apêndice A 63
O que é Sandbox? 63

Apêndice B 64
Relatório Avançado do Sistema 64
Requisitos do Sistema Operacional 65
Internet Explorer 66
Processos 67

Copyright © 1990-2010 Norman ASA

Apresentação

Requisitos do sistema

Esta versão é compatível com a instalação do Conjunto de Segurança Norman v8.00 em computadores com Windows XP, Windows Vista e Windows 7 segundo as especificações a seguir:

Windows		XP	Vista	7
Antivirus		☑	☑	☑
Intrusion Guard		Somente 32 bits	☑	☑
Personal Firewall			☑	☑
Parental Control			☑	☑
Antispam [1)]			☑	☑
Privacy Tools			☑	☑
Service Pack	ou superior	2	1	
CPU (com base em processadores Pentium)	Recomendado	1,8 GHz		
RAM	Recomendado	2 GB		
Internet Explorer	ou superior	7 (8)		
Espaço de disco disponível	Recomendado	500 MB		
Resolução de tela	Recomendado	1024x768		

[1)] O Antispam é compatível apenas com Windows Outlook, Outlook Express e Vista Mail.

Sobre esta versão

A versão atual está disponível em diversos idiomas. Novos idiomas são acrescentados em intervalos regulares. Contate seu distribuidor Norman para obter informações sobre o Conjunto de Segurança em seu idioma. Consulte os websites da Norman para obter detalhes ou contate o distribuidor local para obter informações sobre as versões em outros idiomas.

Sobre este manual

O manual atual apresenta uma visão geral dos produtos, recursos e funções principais do Conjunto de Segurança Norman. Consulte a ajuda on-line para obter explicação detalhada de todas as opções disponíveis.

OBSERVAÇÃO: Observações especiais ou importantes são marcadas com um ponto de interrogação na margem esquerda.

Treinamento e Suporte Técnico

Para obter treinamento ou suporte técnico, contate seu distribuidor local ou a Norman ASA. A Norman oferece suporte técnico e serviços de assessoria para o Conjunto de Segurança e questões de segurança em geral. O suporte técnico também inclui garantia de qualidade da instalação do antivírus, incluindo assistência na personalização do Conjunto de Segurança para atender exatamente às suas necessidades. Tenha em mente que o número de serviços disponíveis varia segundo cada país.

Informações de contato sobre os Escritórios da Norman são apresentadas na última página deste documento.

Copyright © 1990-2010 Norman ASA

O que é o Conjunto de Segurança Norman?

O Conjunto de Segurança Norman (NSS) é um pacote de segurança de software composto de seis diferentes aplicativos de segurança:

☑ **Antivirus e Antispyware**	impedem que o computador seja contaminado por vírus
☑ **Personal Firewall**	impede que hackers utilizem o computador como trânsito para tráfego indesejável
☑ **Antispam**	bloqueia e-mails indesejáveis e em massa
☑ **Parental Control**	impede os jovens de acessar websites com conteúdo indesejável
☑ **Privacy Tools**	ajuda a excluir de forma segura arquivos e dados pessoais.
☑ **Intrusion Guard**	impede que programas maliciosos invadam e infectem o computador

* As duas aplicações mais recentes, Privacy Tools e Intrusion Guard, estão incluídas somente na versão Security Suite PRO.

Norman Security Suite está pronto para uso após a instalação. As opções de configuração padrão fornecem a proteção que você precisa e não é preciso passar pelas opções de configuração para tornar o programa operacional. Entretanto, é proveitoso ter uma noção de como as coisas funcionam e se familiarizar com as funções básicas. Este manual pretende destacar determinados recursos úteis e fornecer algumas sugestões sobre como aproveitar o programa ao máximo.

OBSERVAÇÃO: Você deve executar um assistente antes de iniciar o Personal Firewall. Consulte a seção "Assistente de Instalação" na página 12 , para obter mais informações.

Antivirus & Antispyware

Este programa antivírus monitora seu computador contra softwares maliciosos, também conhecidos como malwares. Os malwares são vírus, worms, cavalos de troia e outras variedades de códigos indesejáveis. O spyware não é destrutivo como os vírus tradicionais, mas as consequências de divulgação inadvertida de informações pessoais podem ser igualmente prejudiciais. O Sandbox exclusivo da Norman fornece proteção proativa que identifica até mesmo vírus desconhecidos.

Para obter mais informações sobre o Sandbox da Norman, consulte a página 63.

Os vírus podem ser removidos automaticamente de discos rígidos, mídias removíveis, anexos de e-mail etc. O aplicativo Antivírus e Antispyware verifica os arquivos no momento em eles são acessados, e possível vírus são removidos automaticamente. O Conjunto de Segurança apresenta dois principais recursos de varredura — a Verificação automática e a Verificação manual — assim como os diferentes métodos de verificação.

Como incentivamos os usuários a executar verificações do computador, você pode iniciar uma verificação de todo o computador – dinamicamente – do menu da bandeja do sistema. É possível também iniciar uma verificação do menu de atalho ao navegar pelos arquivos ou selecionar a proteção de tela que também inicia uma verificação de vírus ao ser ativada. Ao retomar o trabalho e uma verificação for finalizada, ela continuará de onde parou da próxima vez que a proteção de tela for ativada. Para verificações manuais regulares, é possível utilizar o editor de tarefas e o programador para definir qual área da máquina deverá ser verificada e quando.

Este produto é enviado com ajustes pré-selecionados que consideramos adequados para protegê-lo contra ataques de vírus. Os módulos podem ser configurados para que você possa configurar o aplicativo para que ele se adapte exatamente às suas necessidades.

Copyright © 1990-2010 Norman ASA

Personal Firewall

Toda vez que você estiver conectado à Internet, lendo e-mails ou navegando na web, você se conecta a outros computadores de todas as partes do mundo — e eles se conectam ao seu. É por esse motivo que surgem os problemas. Invadindo seu computador, os hackers podem acessar seus documentos particulares, utilizar seu computador para seus próprios atos maléficos ou até mesmo inutilizar seu computador excluindo arquivos importantes do sistema.

Esse aplicativo tem como principal objetivo proteger contra hackers e controlar o tráfego de entrada e de saída do computador com base em uma política de segurança (um conjunto de regras). Essas regras são estabelecidas (automaticamente ou autodefinidas) ao instalar o produto.

O assistente de regras do aplicativo pode criar automaticamente regras para o comportamento dos aplicativos quanto ao acesso à Internet. Há diferentes modos para usuários experientes e inexperientes, e o aplicativo apresenta uma “consciência do modo de servidor”. Você poderá criar e alterar regras bem como visualizar detalhes de tráfego e atividade de portas.

Além disso, o Personal Firewall avançado oferece:

- **Proteção contra reprodução automática,**
  - que detecta as tentativas de um aplicativo de ser iniciado por meio de outro aplicativo.
- **Proteção contra início sigiloso,**
  - que revela aplicativos maliciosos tentando acessar a Internet por meio de outros aplicativos. O Personal Firewall monitora todos os aplicativos principais.
- **Proteção contra “sequestro” de processos,**
  - que evita que aplicativos maliciosos “sequestrem” um processo “confiável” para inserção de .dll ou encadeamento.
- **Modo sigiloso total,**
  - que assegura que todas as portas de seu computador estejam completamente invisíveis externamente.
- **Tratamento avançado de svchost,**
  - no qual cada serviço svchost tem regras separadas em vez de uma regra geral que abranja o grupo de serviços que cada sessão Svchost.exe pode conter.
  - **O Svchost** é um nome genérico de processo de host para serviços no Windows 2000/XP/2003/Vista que vários processos de rede e Internet utilizam para funcionar corretamente. Esse serviço pode executar muitas instâncias simultaneamente, todas necessárias para a operação do computador individual. O serviço tem uma necessidade legítima de acessar a Internet frequentemente, e como qualquer outro aplicativo que se conecta à Internet, é uma função do Firewall Pessoal monitorar e advertir sobre esse tipo de atividade. Enquanto muitos firewalls tem apenas uma regra genérica para manipular svchosts, frequentemente não editáveis, este Firewall Pessoal distingue entre as instâncias diferentes e pode identificar se o processo é conhecido ou desconhecido. Além disso, há opções de configuração para diversos serviços svchost nos arquivos de ajuda do aplicativo.
- **“Anti-pharming”,**
  - implementado por meio da proteção do arquivo de hosts e, portanto, eliminando o método de ataque “pharming” mais comum.
  - A palavra **Pharming** é formada dos termos "phishing" e "farming" (ver Antispam abaixo para uma explicação sobre phishing). É chamado de pharming quando um hacker tenta redirecionar o tráfego do website que você está prestes a visitar para outro website falso. O pharming pode ser realizado pela alteração dos arquivos hosts no computador de destino ou pela exploração de vulnerabilidades no software do servidor DNS. Os servidores DNS (Servidor de Nome de Domínio) são responsáveis pela resolução de nomes de Internet em seu endereço real. Nos últimos anos o pharming e o phishing foram utilizados para roubar informações de identidade on-line. O pharming se tornou uma grande preocupação para empresas que hospedam sites de comércio eletrônico e websites de bancos na internet. Medidas sofisticadas conhecidas como antipharming são necessárias para proteger contra essa grave ameaça.

Copyright © 1990-2010 Norman ASA

Antispam

O aplicativo antispam protege contra e-mails comerciais e em massa não solicitados (spam) que podem conter ameaças para o sistema. O Antispam bloqueia spams, tentativas de phishing e outras ameças geradas por e-mail antes que eles possam chegar ao computador. Você pode criar listas de bloqueio e de permissão para administrar os remetentes de e-mail e o conteúdo que deve ser transferido para seu cliente de e-mail.

Tal como os aplicativos antivírus empregam arquivos de definição de vírus para detectar malwares, as soluções antispam utilizam arquivos de definição para filtrar e-mails não solicitados. Os arquivos de definição de vírus incorporam assinaturas de vírus que determinam se o arquivo está ou não infectado, enquanto as definições antispam utilizam um conjunto de critérios para calcular a probabilidade de um e-mail ser um spam. Os arquivos de definição de spam baseiam a análise de um e-mail no idioma, imagens, cores e links incluídos no e-mail, bem como o e-mail e o endereço IP do remetente. Mesmo assim, nem sempre é possível concluir com absoluta certeza se um e-mail é ou não um spam.

- **Spam**
  - E-mail indesejável, geralmente anunciam algum produto. O spam é geralmente inofensivo, mas pode ser importuno tanto quanto demorado.
- **Phishing**
  - A ação de enviar um e-mail para alguém, fingindo ser um público legítimo ou empresa privada em uma tentativa de coletar informações confidenciais que possam ser utilizadas para usurpação de identidade. O e-mail direciona você para um website onde lhe é solicitado atualizar informações pessoais como números de cartão de crédito ou conta bancária – informações que a organização real já possui. O website é uma farsa, mas aparenta ser um bom negócio e foi criado com o único propósito de roubar informações. O termo 'phishing' é uma variação da palavra 'fishing', onde o trocadilho baseia-se na noção de lançar a isca com as esperanças de que alguém vai fisgar.

Parental Control

A Internet não é necessariamente um bom lugar para se estar, e existem alguns websites que certamente não desejaríamos que os mais jovens da família visitassem. A menos que as crianças e adolescentes estejam sob supervisão constante, provavelmente visitarão websites com conteúdo indesejável — deliberadamente ou não.

Com o Parental Control, você pode bloquear o acesso a determinadas categorias de websites ou até mesmo bloquear todos os sites não aprovados expressamente. Além disso, você poderá restringir o tempo durante o qual um usuário tem autorização para navegar na Internet e definir a hora do dia em que ele poderá acessar a Internet.

Resumindo, você poderá personalizar um perfil para um usuário individual com base em idade ou outros critérios que você desejar considerar.

Privacy Tools

Muitos aplicativos, inclusive o sistema operacional em si, registra a atividade do usuário como arquivos que são abertos, websites visitados e documentos visualizados. Esse é um mecanismo de fácil utilização, que facilita a execução de tarefas; visitar o mesmo jornal on-line ou continuar trabalhando em um documento de texto.

Embora isso seja de fácil utilização, é também uma preocupação de privacidade. Outros usuários desse computador, ou outras pessoas que examinar o computador mais tarde, podem analisar esses registros e descobrir algo que você deseja manter em privacidade. Mesmo se você excluir um arquivo do computador, ele não será completamente destruído. Ferramentas avançadas podem recuperar o arquivo novamente e por isso comprometer documentos delicados. Os registros acompanham a navegação na Internet e a abertura de arquivos no computador.

Essa funcionalidade é uma grande preocupação para sua privacidade. Constituindo um risco potencial de manipulação social e roubo de identidade ou senha. As informações pessoais adquiridas podem, por sua vez, serem utilizadas com intenção maliciosa.

Copyright © 1990-2010 Norman ASA

Com o Privacy Tools você pode excluir arquivos específicos de uma maneira segura. O conteúdo dos arquivos são permanentemente apagados e não pode ser recuperado. É possível também configurar o aplicativo para excluir automaticamente vários arquivos de registros contendo dados pessoais, cookies e histórico do navegador. A exclusão de registros do histórico não afeta as configurações e indicadores do aplicativo.

Intrusion Guard

Este é um sistema de prevenção com base em host (HIPS) que pode impedir aplicativos maliciosos de assumir o controle da máquina. O aplicativo oferece uma poderosa ferramenta de relatório e protege processos, drivers, navegadores e arquivo de hosts. É uma plataforma proativa de proteção contra ameaças direcionada para usuários experientes.

- Ferramenta de Relatório Avançado do Sistema
  - Essa ferramenta eficaz proporciona o controle dos aplicativos instalados, dos filtros de sistema e dos módulos suspeitos descobertos no computador.
- Recursos eficazes em tempo real
  - Esse recurso pode ser configurado para registrar, advertir e bloquear intrusões.
- Proteção de processos
  - Impede aplicativos maliciosos de usurpar (assumir o controle) outros aplicativos e instalar conteúdo mais malicioso no sistema do computador.
- Proteção de driver
  - Interrompe a instalação dos drivers e protege contra outras técnicas maliciosas que obtêm acesso de baixo nível ao sistema do computador.
- Prevenção de usurpação do navegador
  - Monitora as configurações do Internet Explorer e gerencia os cookies. Pode também registrar, advertir e bloquear tentativas de instalação de filtros de rede, como LSP (Provedor de Serviços em Camadas) e BHO (Objeto Auxiliar do Navegador).
- Proteção dos arquivo de hosts
  - Protege o arquivo de hosts de modificações não autorizadas.

Copyright © 1990-2010 Norman ASA

Instalação

Este capítulo abrange os requisitos do sistema, chave de licença, como recuperar o instalador e como instalar o Conjunto de Segurança Norman no computador.

Recuperando o software

Um CD com o instalador foi fornecido no momento da compra do Conjunto de Segurança Norman ou um endereço da página da Web para o download na Internet está incluído na documentação de compra.

CD-ROM

Se você recebeu um CD-ROM da Norman, utilize-o para iniciar a instalação.

1. Insira o CD no drive de CD-ROM.
   - O CD será executado automaticamente e o menu do CD aparecerá. Se o menu do CD não aparecer em um minuto mais ou menos, o recurso Autorun pode estar desativado. Para iniciar o menu do CD manualmente, faça um dos seguintes:
     - Navegue por meio do conteúdo do CD e clique duas vezes no arquivo raiz Norman.exe.
     - Clique em **Iniciar > Executar** e digite D:\Norman.exe. Substitua D: pela letra de partição real de seu drive de CD-ROM. Clique em **OK**.
2. Escolha o idioma para visualização do menu do CD.
3. Selecione o idioma de instalação a partir da página de **Instalação** do menu do CD.

O Assistente InstallShield é iniciado. Avance para “Instalação” na página 10.

Download na Internet

O instalador pode ser baixado da Internet. O local da Internet e procedimento de download é descrito nas informações do pedido de compra. Se não for o caso, siga as instruções abaixo para fazer o download do instalador e iniciar a instalação.

1. Abra seu navegador da Internet e digite o endereço geral na Web para downloads de software da Norman: **http://www.norman.com/downloads/**
2. Selecione o instalador Conjunto de Segurança Norman pelo idioma e/ou versão.

OBSERVAÇÃO: Escolha o instalador correto segundo seu computador 64 ou 32-bits.

3. Clique em **Salvar**, ou **Executar**.

   a) **Salve**

   Se clicar em **Salvar** você terá permissão para salvar o arquivo no computador e instalá-lo a partir do local onde foi salvo. Uma conexão com a Internet não é necessário ao instalar do computador. Entretanto, recomendamos uma conexão com a Internet durante a instalação para validação da chave e atualização.
   - Navegue por um local da pasta para salvar o instalador e, em seguida, clique em **Salvar** para confirmar.
     - Anote o local onde você salvou o instalador.
     - Como a janela de download, o navegador não é mais necessário e pode ser fechado também.
   - Localize o instalador e clique duas vezes no arquivo.
     - O instalador pode ser excluído após uma instalação bem-sucedida, ou você pode salvá-lo em uma mídia externa para backup.

   b) **Executar**

   Clique em **Executar** para iniciar a instalação diretamente da web. O instalador baixa e, em seguida, inicia automaticamente a instalação do produto. Se instalação falhar, você deve visitar a página de download novamente.

O Assistente InstallShield é ativado. Avance para “Instalação” na página 10.

Copyright © 1990-2010 Norman ASA

Chave de licença

Ao comprar o Norman Security Suite você recebe uma chave de licença do produto. A chave é necessária para a instalação a ser atualizada. Um software antivírus que não é atualizado regularmente não cumpre seu propósito.

Tenho uma chave

Você deve digitar a chave durante a instalação, quando solicitado pelo Assistente InstallShield. O aplicativo procurará automaticamente as atualizações assim que a instalação for finalizada.

Não tenho uma chave

Você pode deixar o campo chave em branco e, mesmo assim, instalar o pacote completo. Entretanto, o Assistente de Licença lhe solicitará regularmente uma chave e o(s) produto(s) não será(ão) atualizado(s).

Digite uma chave após a instalação ser finalizada

Você pode ativar o Assistente de Licença do aplicativo e colar a chave no campo apropriado. Consulte a seção “Assistente de Licença” na página 58.

Instalação

Execute o Assistente InstallShield do Conjunto de Segurança Norman (o instalador). Consulte “Recuperando o software” na página 9 sobre como obtê-lo. Siga as instruções da tela. Clique em **Retornar** se você precisar revisar ou alterar as configurações de instalação.

O local padrão para instalação é `C:\Arquivos de Programas\Norman`**.**

1. A tela de boas-vindas do Assistente InstallShield aparece. Clique em **Avançar**.
2. Leia o contrato de licença e aceite-o para continuar a instalação. Clique em **Avançar**.
3. Digite uma chave de licença do produto válida. Clique em **Avançar**.
   - A chave contém informações sobre os produtos que você comprou.
   - Você pode deixar o campo vazio se apenas quer avaliar o produto. Recomenda-se digitar uma chave de avaliação para aproveitar ao máximo o produto durante o período de avaliação.

DICA

COPIE E COLE A CHAVE DE LICENÇA. Caso tenha uma cópia de sua chave de licença em um e-mail ou algum outro formato eletrônico, a maneira mais fácil é copiar a chave no campo chave de licença. Realce a chave e pressione **Ctrl+C**, posicione o cursor no campo chave de licença e pressione **Ctrl+V** para colar na chave. Verifique se não há espaços em branco.

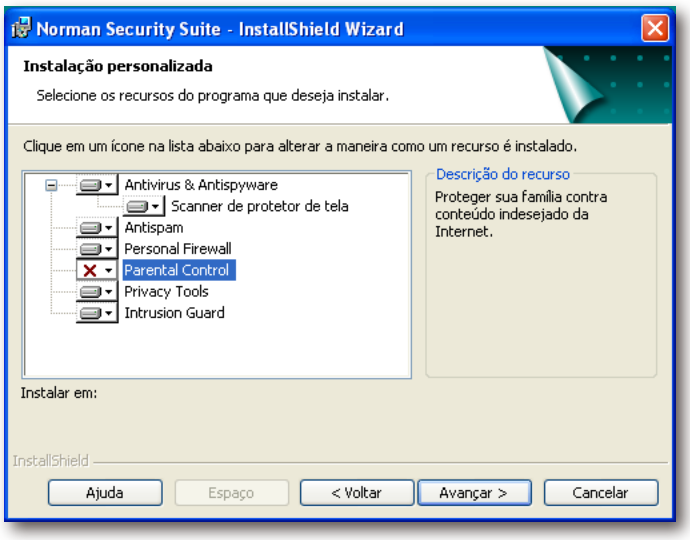
OBSERVAÇÃO: Caso não possua uma chave, você pode deixar este campo em branco e, ainda assim, instalar todo o conjunto. Entretanto, o Assistente de Licença lhe solicitará regularmente uma chave e o(s) produto(s) não será(ão) atualizado(s). Se necessário, o Assistente de Licença o ajudará a obter uma chave em um ponto posterior.

4. **Tipo de instalação**
   a) Selecionar **Concluir** instalará todos os recursos do programa para o local padrão.
      - Selecione **Concluir** e clique em **Avançar**
      - Avance para o ponto “7. Pronto para instalar.” abaixo.

   b) Selecione **Personalizar** para decidir quais produtos instalar e/ou selecionar ou local diferente do local padrão.
      - Selecione **Personalizar** e clique em **Avançar**.
5. **Instalação personalizada**
   Uma lista de produtos que você pode instalar é exibida.
   - **Antivirus & Antispyware**
     - **Scanner de protetor de tela**
   - **Antispam**

Copyright © 1990-2010 Norman ASA

- **Personal Firewall**
- **Parental Control**
  - Você precisa selecionar este produto manualmente se desejar instalá-lo. Clique no menu suspenso à esquerda para selecionar a instalação desse recurso no disco rígido local. A instalação deste produto exige a chave de licença ou parte de uma instalação de avaliação.
  - Além disso, se preferir, você pode instalar este produto posteriormente.
- **Privacy Tools**
- **Intrusion Guard**



  - Clique em **Espaço** se desejar ver o espaço em disco necessário para as instalações selecionadas.
    - Clique em **OK** para retornar a exibição **Configuração Personalizada**.
  - Clique em **Avançar** para continuar.

6. **Pasta de destino**

   a) Clique em **Avançar** se desejar instalar os aplicativos selecionados para o local padrão.

   b) Clique em **Alterar...** para definir outro local.
   - Selecione o local da lista suspensa, adicione uma nova pasta ou digite um caminho no campo de entrada de nome de pasta.
   - Clique em **OK** para confirmar e retornar à exibição da pasta de destino.
   - Clique em **Avançar**

7. Pronto para instalar.
   - Clique em **Instalar** para começar a instalação.
8. Instalando o Norman Security Suite.
   - Surgirá uma caixa de diálogo informando que o aplicativo agora está pronto para ser iniciado e para configurar os componentes instalados. Clique em **OK** para continuar.
9. Surgirá a caixa de diálogo de conclusão: Clique em **Finalizar** para concluir o **Assistente InstallShield**. A instalação continuará a ser executada em segundo plano por 5 a 10 minutos.
10. Clique em **Reiniciar agora** quando lhe for solicitado reiniciar o computador. Após reiniciar um formulário de registro de cliente e – caso o Personal Firewall seja instalado – o Assistente de Instalação do Personal Firewall é iniciado.
    - **Informações de Cliente**
      - Digite as informações necessárias e, depois, clique em **Enviar**.
    - **Assistente de Instalação**
      - Consulte a próxima seção.

Copyright © 1990-2010 Norman ASA

Assistentes

O Norman Security Suite possui três assistentes diferentes. Eles gerenciam a instalação e as configurações básicas do produto.

Assistente InstallShield
Este assistente permite a instalação o Norman Security Suite. O assistente é também conhecido como o instalador ou arquivo de instalação.

Assistente de Instalação
Este é importante quando o Personal Firewall é instalado. Quando a instalação do Norman Security Suite com o Personal Firewall é instalado, um assistente para configuração do Personal Firewall é iniciado. Consulte a próxima seção.

Assistente de Licença
Este assistente ajuda a rastrear licenças válidas de produto. Consulte a seção “Assistente de Licença” na página 58

Assistente de Instalação

Você concluiu a instalação do Norman Security Suite (Cf. “Instalação” na página 10), e o Personal Firewall é um dos recursos instalados. O Assistente de Instalação é iniciado automaticamente.

Este assistente permite estabelecer regras básicas automaticamente, como permissão de acesso à Internet para aplicativos relevantes. A finalidade é identificar programas que necessitam de autenticidade para acessar a Internet e criar regras para esses aplicativos. Recomenda-se enfaticamente executar o assistente de instalação. Depois, você sempre poderá alterar, de maneira automática, as regras geradas, utilizando o Editor de Regras.

Se optar por não executar o Assistente de Instalação, o computador pode não se conectar à Internet e aplicativos importantes são serão atualizados. Consulte a seção “Ferramentas de Perito” na página 33.

1. Leia a página de introdução e clique em **Avançar**.
   O Assistente de Instalação oferece etapas diferentes para usuários experientes e inexperientes. O usuário experiente pode especificar determinados detalhes, enquanto o usuário inexperiente é guiado pelas configurações automáticas.
2. Avalie seu nível de experiência e clique em **Avançar**.

   Usuário inexperiente
   - Usuário com conhecimentos básicos de Internet sem perícia ou interesse nos aspectos técnicos de computadores. O firewall tomará as decisões para você e manterá sua interação com o programa apenas nos aspectos básicos.
   - Selecione o nível de segurança para gerenciamento de conexões com a Internet que tentam acessar o computador (tráfego de entrada) ou aplicativos que tentam conectar-se à Internet (tráfego de saída).
     - **Modo básico**.
       - Todo o tráfego é permitido, a menos que uma regra permanente evite a conexão. Você estará protegido contra ataques do tráfego de entrada.
     - **Modo normal**.
       - Você será solicitado para o tráfego desconhecido, o qual deverá permitir ou negar, a menos que uma regra permanente evite a conexão. Você será protegido contra ataques do tráfego de entrada e de aplicativos indesejáveis que envia dados de seu computador.

   Usuário experiente
   - O usuário que está familiarizado com as configurações comuns do firewall e entende o que é endereço IP e número de porta. O firewall oferece mais opções avançadas durante a configuração e uso.
3. Siga as instruções na tela em questão para adicionar outros navegadores ou clientes de e-mail, configurando recursos de rede (configuração avançada, se for selecionado usuário experiente), e permitir outros aplicativos conhecidas.
4. Por fim, clique em **Finalizar** para concluir o assistente.

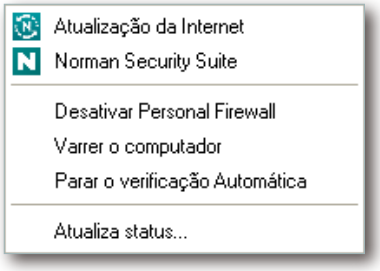
Copyright © 1990-2010 Norman ASA

Guia de Introdução

Ícone da bandeja do aplicativo

Durante a configuração, um ícone é colocado na bandeja do sistema no canto inferior direito da tela. Esse ícone confirma que o Security Suite está instalado na máquina.

Ao clicar com o botão direito do mouse no ícone o menu da bandeja do sistema do Security Suite é exibido.



Os itens da lista com um ícone na frente deles são cópias dos itens que aparecem a qualquer momento no menu **Iniciar > Programas > Norman Security Suite**. Este é um atalho para os principais módulos do Norman Security Suite, assim como algumas tarefas típicas.

- **Atualização da Internet**
  - Ative o recurso Atualização da Internet e atualize os produtos instalados.
- **Norman Security Suite**
  - Abra o aplicativo Norman Security Suite.
- **Desativar o Personal Firewall (Ativar o Personal Firewall)**
  - Alterna entre ativar e desativar o Personal Firewall.
- **Verificação do computador**
  - Iniciar uma verificação manual de todo o computador.
- **Interromper verificador automático (Iniciar verificador automático)**
  - Alterna entre iniciar e interromper a verificação automática.
- **Status da atualização...**
  - Visualizar status da atualização para os produtos instalados. Essa função, além disso, é a originadora de mensagens relacionadas com arquivos de definição de vírus desatualizados, vencimento de período de licença e outras informações.

OBSERVAÇÃO: As opções do menu diferem dependendo dos produtos instalados. Por exemplo, a opção Ativar ou Desativar Personal Firewall é apenas visível quando o Personal Firewall é instalado.

Copyright © 1990-2010 Norman ASA

Os ícones de aviso da bandeja

O ícone da bandeja Norman também fornece informações relacionadas com o status da instalação do Security Suite. Coloque o cursor no ícone da bandeja para uma explicação de qualquer erro ou mensagem

Círculo vermelho

Esse ícone indica que alguns dos componentes atualmente em execução estão desatualizados. Se o ícone aparecer com o símbolo vermelho intermitente, posicione o dispositivo indicador sobre o símbolo para saber qual componente precisa de atualização ou se existem outras situações de erro.

OBSERVAÇÃO: Durante a inicialização, o símbolo vermelho ficará visível até que todos os módulos sejam iniciados. Quando mais antigo e lento for o computador, mais tempo leva para carregar todos os módulos. Contudo, o ícone normal do Norman deve aparecer após, no máximo, 1 a 2 minutos.

Triângulo amarelo

O ícone de triângulo amarelo, constante ou intermitente, significa que a verificação automática foi desativada manualmente, o aplicativo está aguardando para ser reiniciado, uma erro de instalação ocorreu ou os arquivos de definição estão desatualizados.

- **Constante**
  - A verificação automática foi desativada manualmente nas configurações do aplicativo. Consulte a seção “Ativar verificador automático” na página 23.
  - O aplicativo está aguardando para ser reiniciado. A opção **Reiniciar mais tarde** pode ter sido selecionada em uma tela anterior.
  - Ocorreu um possível erro de instalação. Tente reiniciar o computador para resolver o possível erro.

- **Intermitente**
  - Os arquivos de definição de vírus estão desatualizados. Isso significa que estão, pelo menos, dez dias desatualizados.
  - A verificação automática foi interrompida a partir do menu da bandeja do sistema. Clique com o botão direito no ícone da bandeja do sistema. Selecione **Iniciar verificador automático**.
  - O firewall foi desativado. Clique com o botão direito no ícone da bandeja do sistema. Selecione **Desativar Firewall**.

Roda de engrenagem

Quando o ícone da bandeja aparece com uma engrenagem, o Gerenciador de Programas da Norman está funcionando com o programa, muito provavelmente com uma atualização. Recomendamos não desligar a máquina quando o NPM estiver em funcionamento, isto é, enquanto esse símbolo estiver visível.

OBSERVAÇÃO: Uma atualização não deve levar mais que 5 ou 10 minutos. Se o ícone da engrenagem estiver visível por um longo período, algum erro pode ter ocorrido com a instalação. Nesse caso, tente reiniciar o computador. Se isso não finalizar o ícone de engrenagem, então, tente a opção de reparo descrita na seção “Reparo automático” na página 61.

Símbolo da Central de Segurança do Windows

A Norman é um dos fornecedores de antivírus detectados pelo sistema operacional. Se os arquivos de definição de vírus estiverem desatualizados ou se a Verificação automática não estiver sendo executada, você também receberá uma mensagem de advertência do Windows de que algum erro ocorreu. O símbolo da Central de Segurança aparece e você pode clicar nele para visualizar e editar as configurações do Windows.

Copyright © 1990-2010 Norman ASA

Abrir o aplicativo

Você pode abrir o aplicativo via menu da bandeja do sistema ou via menu do Windows. Clique com o botão direito do mouse no ícone da bandeja do sistema do aplicativo e selecione **Norman Security Suite** do menu suspenso. A partir do menu do Windows, clique em **Iniciar** e selecione **Todos os programas > Norman Security Suite > Norman Security Suite**.

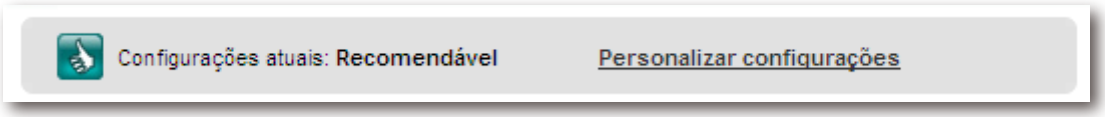
Ícones de aviso do produto

Algumas vezes, um triângulo amarelo aparece na entrada do menu do aplicativo. O motivo disso pode ser que um produto esteja desativado ou desatualizado, a licença expirou, um software instalado recentemente precisa d de configuração final para finalizar seu procedimento de instalação etc. Selecione a entrada do menu com aviso para descobrir mais.

OBSERVAÇÃO: Ao abrir o Security Suite pela primeira vez, um aviso é emitido para o aplicativo Parental Control. Consulte a seção "Parental Control" na página 44

Configurações do Security Suite

Este aplicativo está instalado com as configurações padrão recomendadas para uso diário. Você pode selecionar **Personalizar configurações** da página de produtos do aplicativo para configurar os produtos por meio de uma séria de opções diferentes. Ao alterar de uma configuração para outra, observe a mudança no ícone e que a o texto inicial das configurações muda de local.



- Configurações atuais: **Recomendado**
  - As configurações padrão são eficazes, conforme recomendado para uso diário.
  - Clique em **Personalizar configurações** se desejar alterar as configurações padrão.

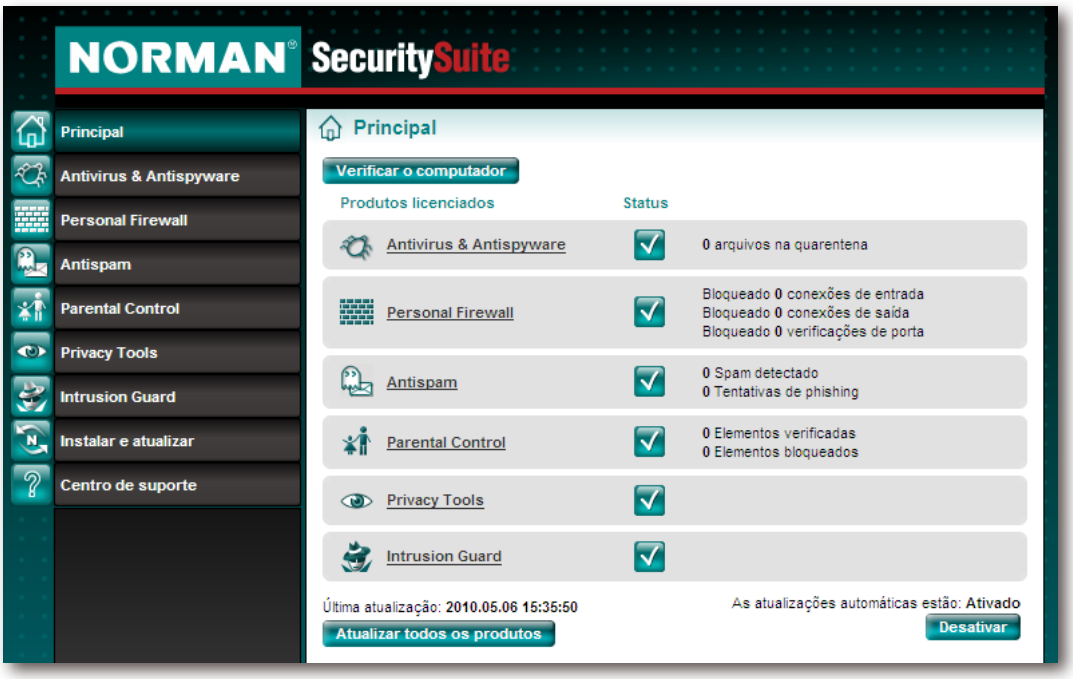
- Configurações atuais: **Personalizar**
  - As configurações padrão são ou podem ser personalizadas.
  - Clique em **Utilizar configurações recomendadas** para redefinir as configurações para padrão.

OBSERVAÇÃO: Recomenda-se não alterar as configurações padrão a menos que você saiba como as alterações afetam o sistema. Assegure-se de que personalizar as configurações não leve a um nível de segurança inferior. Se tiver dúvidas, lembre-se de que as configurações padrão oferecem proteção suficiente

Copyright © 1990-2010 Norman ASA

Página Principal

Abra o aplicativo Security Suite para visualizar o status dos produtos instalados. Consulte o “Guia de Introdução” na página 13 sobre como abrir o aplicativo.



Execute uma verificação do computador, monitore quais produtos são instalados e visualize algumas informações detalhadas sobre eles. Atualize todos os produtos e altere as atualizações automáticas de on (ativada) ou off (desativada) com um clique.

Clique em **Verificar Computador** para iniciar uma verificação manual de todo o computador. Essa verificação utiliza as mesmas configurações conforme especificado para a Verificação Manual. Consulte “Verificador manual” na página 25.

Os **Produtos licenciados** são os cobertos pela chave de licença do produto. Consulte a seção “Chave de licença” na página 10. O ícone de status indica se a instalação está atualizada e completa, se é necessário atualizar ou se um produto não está instalado. As estatísticas à direta exibem os dados dos aplicados em funcionamento.

OBSERVAÇÃO: Ao abrir o Security Suite pela primeira vez, um aviso é emitido para o aplicativo Parental Control. Consulte a seção “Parental Control” na página 44

Atualizar todos os produtos

Atualize todos os produtos instalados com apenas um clique. Para configurações adicionais e visão geral, consulte “Instalar e atualizar” na página 57.

As atualizações automáticas estão ativadas (on)/desativadas (off)

Os produtos serão atualizados regularmente quando as atualizações automáticas estiverem ativadas (on). Editar configurações de “Selecionar o método de atualização” na página 58.

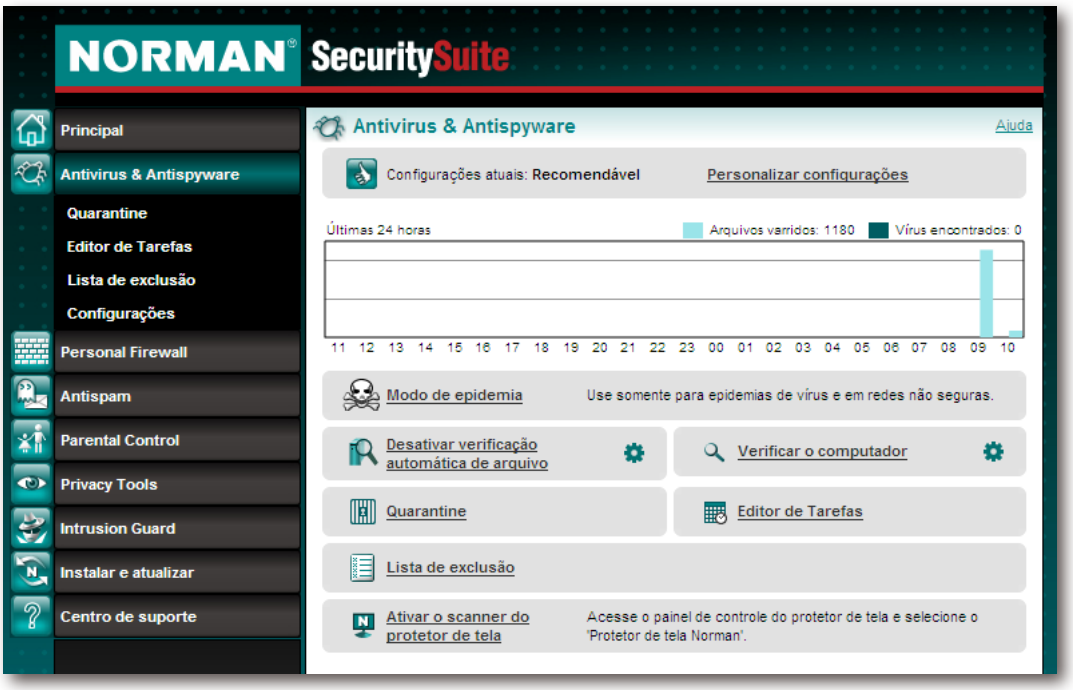
OBSERVAÇÃO: Recomendas enfaticamente que as atualizações automáticas estejam sempre ativadas

Copyright © 1990-2010 Norman ASA

Antivirus & Antispyware

Abra o aplicativo Security Suite e selecione **Antivirus & Antispyware** do menu do lado esquerdo. Consulte o “Guia de Introdução” na página 13 para obter instruções de como abrir o aplicativo e para 5 uma descrição da finalidade e função do aplicativo.

Visualização principal


NORMAN SecuritySuite
Principal
Antivirus & Antispyware
Quarantine
Editor de Tarefas
Lista de exclusão
Configurações
Personal Firewall
Antispam
Parental Control
Privacy Tools
Intrusion Guard
Instalar e atualizar
Centro de suporte
Antivirus & Antispyware
Ajuda
Configurações atuais: Recomendável
Personalizar configurações
Últimas 24 horas
Arquivos varridos: 1180
Vírus encontrados: 0
11 12 13 14 15 16 17 18 19 20 21 22 23 00 01 02 03 04 05 06 07 08 09 10
Modo de epidemia
Use somente para epidemias de vírus e em redes não seguras.
Desativar verificação automática de arquivo
Verificar o computador
Quarantine
Editor de Tarefas
Lista de exclusão
Ativar o scanner do protetor de tela
Acesse o painel de controle do protetor de tela e selecione o 'Protetor de tela Norman'.

Este programa antivírus e antispyware monitora seu computador contra softwares maliciosos, também conhecidos como malwares. Este capítulo trata da configuração das duas principais verificações de vírus – a verificação automática e a verificação manual – bem como da administração de arquivos em quarentena, agendamento de exames, ativação do verificador da proteção de tela e da habilitação do recurso antispyware.

Personalizar configurações

Clique nesta opção para editar os valores padrão. Consulte a seção “Configurações” na página 22. Para obter informações gerais sobre selecionar configurações recomendadas versus configurações personalizadas, consulte “Configurações do Security Suite” na página 15.

Estatísticas de varredura

A página principal do aplicativo exibe uma representação gráfica de arquivos verificados e infectados nas últimas 24 horas. Os números estatísticos representam a atividade das verificações automáticas e manuais.

Modo de ocorrência

Esse recurso deverá ser ativado apenas temporariamente em caso de desencadeamento de vírus e ao conectar-se à redes sem fio desconhecidas e inseguras. Ativar essa opção pode afetar o desempenho e a estabilidade.

Desativar verificação automática de arquivo

Consulte a seção **Configurações > Verificação automática ativada na** página 23.

Copyright © 1990-2010 Norman ASA

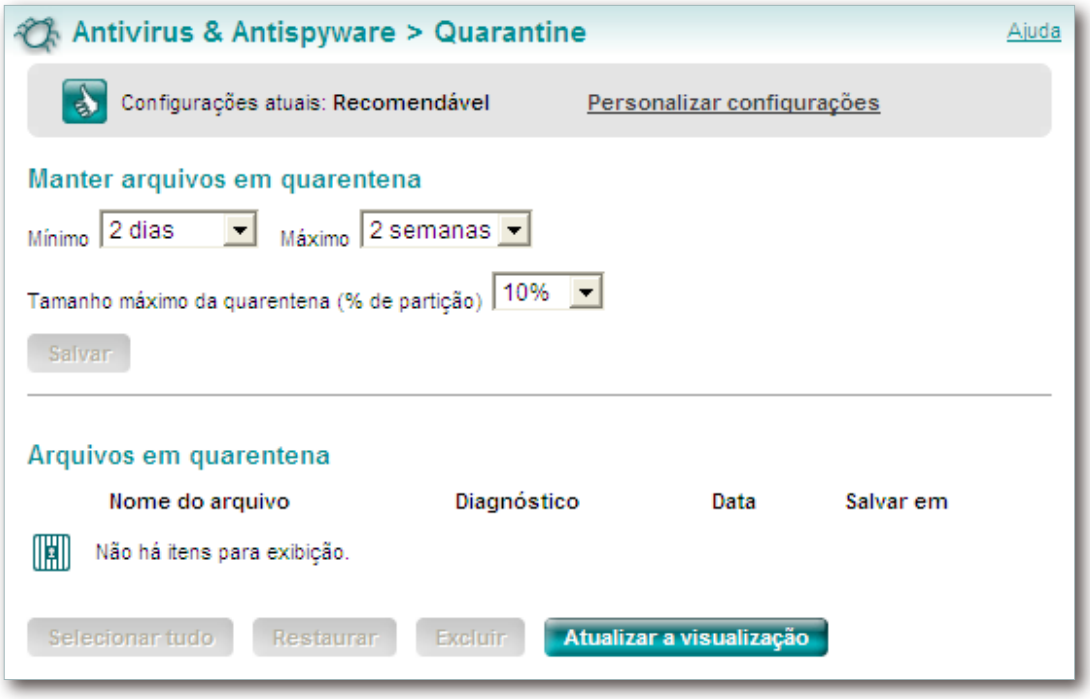
Verificação do computador

A verificação manual inicia um exame de todos os discos rígidos no sistema. A partir da caixa de diálogo de verificação que aparece é possível selecionar **Interromper** se você desejar **Navegar** para outro local para executar verificação.

É possível também iniciar essa verificação do menu da bandeja do sistema. Clique com o botão direito do mouse sobre o ícone da bandeja do aplicativo e selecione **Verificar computador**.

Consulte “Verificador manual” na página 25 sobre como configurar o verificador manual.

Quarentena



Manter arquivos em quarentena

Selecione **Personalizar configurações** para acessar as opções de configuração. Especifique o tempo mínimo e máximo que os arquivos devem permanecer em quarentena e quanto espaço em disco eles poderão ocupar.

- **Mínimo**
  Especifique um período variando de um dia a uma semana. Arquivos mais recentes do que o tempo mínimo especificado nunca serão excluídos.
- **Máximo**
  Especifique um período variando de uma a quatro semanas. Arquivos mais antigos do que o tempo máximo serão excluídos sem aviso.
- **Tamanho máximo da quarentena (% de partição)**
  Especifique quanto espaço de disco da partição atual que os arquivos em quarentena poderão ocupar.

OBSERVAÇÃO: O tamanho máximo pode ser excedido no caso em que os arquivos em quarentena ainda estão para alcançar o tempo mínimo especificado.

- Clique em **Salvar** para confirmar as alterações.

Copyright © 1990-2010 Norman ASA

Arquivos em quarentena

Os arquivos infectados que foram colocados em quarentena aparecem nessa lista na caixa de diálogo **Arquivos em quarentena** desde que você tenha configurando o programa a fazer isso. O aplicativo antivírus tentará reparar os arquivos infectados antes que sejam excluídos e/ou colocados em quarentena (dependendo de sua configuração). Os arquivos em quarentena estão infectados ou foram bloqueados pelo recurso de Proteção da Internet.

OBSERVAÇÃO: Por padrão, uma cópia de um arquivo excluído ou bloqueado é colocada em quarentena.

Uma cópia de um arquivo infectado e em quarentena é excluída, a menos que ela esteja em outra pasta, em cujo caso é removida para a quarentena. Quanto a Verificação automática detecta que `C:\eicar.com` está infectado, ele é movido para a quarentena. No entanto, se a Verificação automática detectar `C:\Cópia de eicar.com` e esse arquivo for idêntico a `eicar.com`, ele não será colocado em quarentena, mas excluído. Se a `Cópia de eicar.com` estiver em `C:\outra pasta\` ela será, entretanto, movida para a quarentena por causa da nova localização. Esse método é implementado para evitar que a quarentena seja sobrecarregada em uma situação onde um vírus gravou diversas cópias do mesmo arquivo para a mesma área da unidade de disco.

Um arquivo pode ser colocado em quarentena porque o aplicativo Antivírus suspeita que ele esteja infectado. Raramente e após uma atualização dos arquivos de definição, o Antivírus pode estabelecer que um arquivo previamente em quarentena está finalmente limpo. Como os tipos e técnicas tanto para criar como para detectar vírus mudam rapidamente, o Antivírus verificará a quarentena após uma atualização e após o computador ser reiniciado.

Se um arquivo em quarentena for "absolvido" após essa verificação, ele será restaurado com tanto que haja uma caminho de arquivo válido e se nenhum outro arquivo com o mesmo nome existir. Nenhuma intervenção do usuário é necessária e este não será informado sobre uma possível restauração do arquivo em quarentena.

Editor de Tarefas

Algumas vezes é conveniente definir tarefas que devem ser executadas diversas vezes e/ou em intervalos regulares. A verificação de vírus é uma bom exemplo de uma tarefa que precisa ser executada regularmente e o Editor de tarefas é a ferramenta fornecida para essa finalidade.

É possível criar um arquivo de tarefa para verificações que você deseja executar repetidamente ou para verificações especiais que você pretende executar em determinadas situações. Por exemplo, se você baixa arquivos da Internet para áreas designadas, é possível criar um arquivo de tarefa que verifique apenas essas áreas e execute a tarefa manualmente após os downloads. Além disso, é possível agendar a tarefa a executada em um horário pré-definido.

Os administradores podem criar arquivos de tarefa e distribuí-los para todas as estações de trabalho na rede a fim de garantir uma verificação consistente das áreas que exigem atenção especial.

OBSERVAÇÃO: O diálogo Criar tarefa aparece na primeira vez que você acessar o Editor de Tarefas ou se uma tarefa ainda não foi criada.

Todas as tarefas existentes são exibidas como uma lista no diálogo do Editor de Tarefas.

Copyright © 1990-2010 Norman ASA

Criar uma tarefa

1. Digite um **Nome de tarefa**.
2. Selecione **Verificar todo o computador** ou **Verificação arquivos e pastas infectados**.
   - Clique no símbolo de pesquisa da pasta para navegar pelos arquivos e pastas.
     - Todas as unidades locais são listadas com uma funcionalidade do Windows Explorer.
     - Clique na letra da unidade para procurar diretórios ou arquivos.
     - Se você selecionar arquivos e pastas específicos, todas as subpastas na unidade/pasta selecionada serão automaticamente selecionadas. Você pode desmarcar a opção para subpastas que não deseja incluir.
   - É possível também digitar um caminho e o nome do arquivo ou diretório diretamente no campo de texto de entrada.
     - O asterisco (*) é aceito como caractere curinga, por exemplo, C:*.* para verificar a toda a unidade C:.
     - Coloque o caractere curinga no começo ou no fim do termo pesquisado. Não posicione o caractere curinga no meio do termo de pesquisa
   - Ao clicar em **Adicionar** para salvar, a área específica é adicionada à lista de tarefas.
3. Selecione uma ou mais opções de verificação. **Verificar setores de boot**, **Verificar arquivos** e **Verificar memória** são todos pré-selecionados. Além dessas alternativas, são utilizadas as opções de verificação para a Verificação manual.
   - **Verificar setores de boot**
     - Ao selecionar esta opção, o aplicativo antivírus verificará o setor de boot da(s) área(s) que está(ão) sendo verificada(s).
   - **Verificar arquivos**
     - Selecione esta opção para incluir arquivos arquivados na verificação. Atualmente, há suporte para os seguintes formatos: ACE, APPLE_SINGLE, ARJ, BZIP2, CAB, GZ, LZH, MAIL, RAR, RAR3, SFXZIP, TAR, ZIP e 7Z.
   - **Verificar a memória**
     - Ao verificar a área de memória, o Antivírus e Antispyware procura por vírus residentes. Você deveria se certificar de que não haja vírus na memória.

Copyright © 1990-2010 Norman ASA

Programar verificações

4. Selecione a frequência, hora e data para executar a verificação. A data e hora sugerida é a atual (de acordo com a informação de seu sistema). É possível selecionar outro horário.
5. Por padrão, a tarefa de verificação está **Ativada**. Remova a marca de seleção para desativá-lo.
6. Clique em **Criar**.

Todas as tarefas existentes são exibidas como uma lista no diálogo do **Editor de Tarefas**. É possível visualizar, editar, executar e excluir os arquivos de tarefa a partir do diálogo do Editor de Tarefas. A partir daqui, você pode ativar e desativar ou excluir tarefas. Desmarque a caixa de seleção **Ativar** para desativar uma tarefa. Selecione a caixa de seleção **Excluir** e clique em **Excluir item(s) selecionado(s)** para excluir uma tarefa.

O local padrão para armazenar arquivos de tarefas é `...Arquivo de programas\Norman\Tarefas`.

Remover uma tarefa

Para remover uma tarefa selecione uma entrada na lista de tarefas e clique em **Excluir item(s) selecionado(s)**.

Lista de exclusão

Os arquivos na lista de exclusão não são verificados. Os motivos para não verificar determinados arquivos podem ser pelo acionamento de falso alarme e por terem alto consumo de tempo para serem verificados De qualquer forma, recomendamos verificar arquivos na lista de exclusão ao executar verificações manuais ou programadas.

Copyright © 1990-2010 Norman ASA

OBSERVAÇÃO: As listas de exclusão devem ser tratadas com muito cuidado, por representarem um risco potencial de segurança. Observe que excluir arquivos ou áreas da verificação é uma decisão com risco de segurança.

Utilizar a lista de exclusão

Selecione esta opção para ativar a lista de exclusão. A **Lista de exclusão** é usada para excluir arquivos que podem conflitar com as verificações, afetando o desempenho de seu computador.

Excluir arquivos e pastas da verificação

Especifique arquivos, diretórios ou toda uma unidade que não deseja que seja varrida para detectar malware. Siga estas etapas para excluir itens da verificação:

- Clique no símbolo de pesquisa da pasta, se desejar navegar pelos arquivos e pastas ou digite um nome de arquivo, diretório ou letra de unidade no campo de entrada.

  Cartões curinga (*/?) são aceitos. Coloque o caractere curinga no começo e no fim do termo pesquisado. Não coloque o caractere curinga no meio do termo pesquisado.

OBSERVAÇÃO: NÃO use apóstrofes, “ ou ‘ ao especificar itens para exclusão.

Exemplos

C:\Diretório	Exclui todos os arquivos no diretório e subdiretórios
*.xyz	Exclui todos os arquivos com a extensão .xyz
exemplo.exe	Exclui o arquivo especificado a despeito de onde seja encontrado
C:\System\xyz.doc	Exclui este determinado arquivo

- Especifique qual das verificações, se houver, deve utilizar a lista de exclusão.
- Clique em **Adicionar à lista** para adicionar a entrada na lista de exclusão.

OBSERVAÇÃO: O Security Suite não verifica se os arquivos, pastas ou unidades que você adicionou à lista de exclusão existem de fato. Preste bem atenção ao digitar os nomes e caminhos corretos.

Unidades de rede

Selecione excluir unidades de rede se você não deseja verificar partes às quais tem acesso nos computadores remotos. Especifique para qual dos verificadores, se houver.

Excluir selecionado

Para remover entradas da lista, selecione a entrada relacionada e clique em **Remover item(s) selecionado(s)**. Clique em **Salvar** para confirmar as alterações.

OBSERVAÇÃO: Recomendamos revisar com regularidade as listas de exclusão.

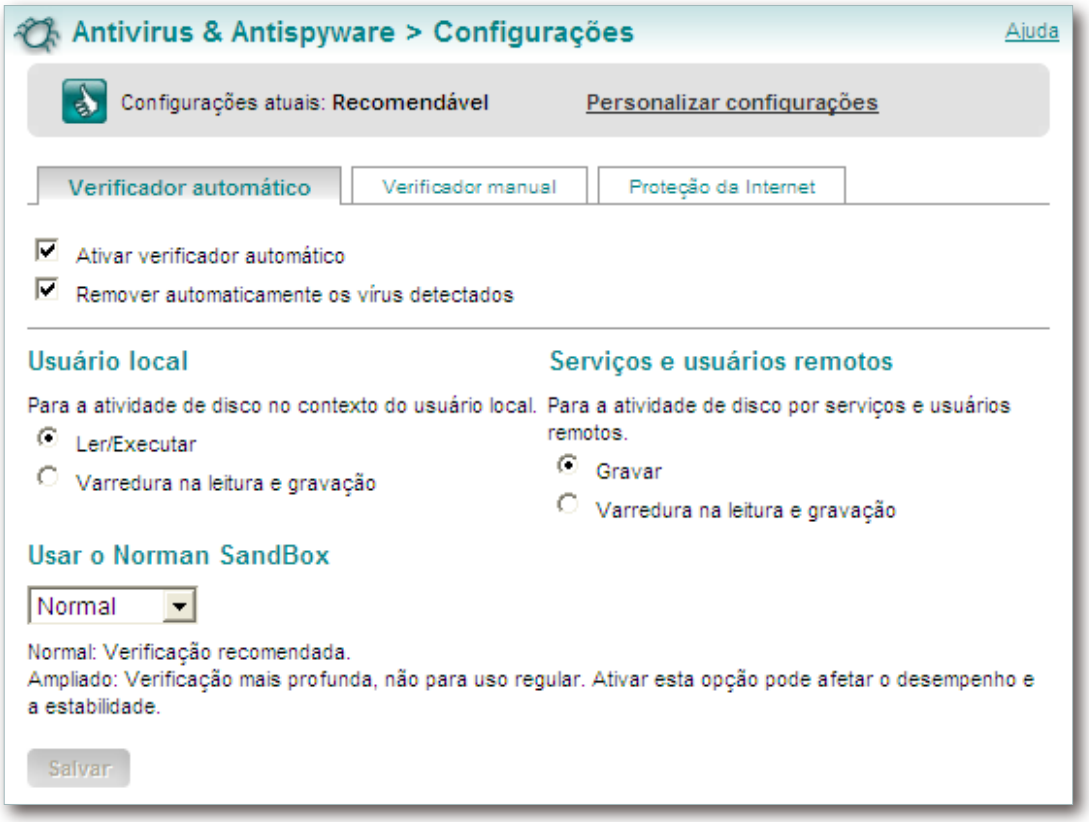
Configurações

A partir dessa seção é possível configurar a verificação automática, a verificação manual e o recurso de Proteção da Internet. Tanto o verificador automático como o manual utilizam, por padrão, o Norman Sandbox. Leia mais sobre o Sandbox em “O que é Sandbox?” na página 63. As configurações do verificador manual são igualmente relevantes para a opção **Verificar computador,** verificar com o botão direito do mouse, Verificar com a proteção de tela e verifica em Linha de comando.

Copyright © 1990-2010 Norman ASA

Verificador automático

A Verificação automática funciona em segundo plano e oferece proteção automática ao seu sistema. Ele é um componente essencial de controle de vírus e deve, portanto, estar sempre ativado.


Antivirus & Antispyware > Configurações
Ajuda
Configurações atuais: Recomendável
Personalizar configurações
Verificador automático
Verificador manual
Proteção da Internet
Ativar verificador automático
Remover automaticamente os vírus detectados
Usuário local
Para a atividade de disco no contexto do usuário local.
Ler/Executar
Varredura na leitura e gravação
Serviços e usuários remotos
Para a atividade de disco por serviços e usuários remotos.
Gravar
Varredura na leitura e gravação
Usar o Norman SandBox
Normal
Normal: Verificação recomendada.
Ampliado: Verificação mais profunda, não para uso regular. Ativar esta opção pode afetar o desempenho e a estabilidade.
Salvar

Ativar verificador automático

A seleção ou o cancelamento da seleção desta opção interrompe e inicia a verificação automática. Recomendamos que a Verificação automática esteja sempre ativada.

Se a Verificação automática for interrompida/pausada no menu da bandeja, aparece um triângulo amarelo intermitente no ícone da bandeja do sistema. Consulte “Ícone da bandeja do aplicativo” na página 13. Além disso, a Central de Segurança do Windows alertará que "Seu computador pode estar em risco".

1. A partir do menu de configurações da Verificação automático, assegure-se de que a opção **Ativar verificação automática** esteja selecionada. Clique em **Salvar** para confirmar as alterações.
   - Desmarque a caixa de seleção para desativar a verificação automática.
   - O Norman Security Suite não emite nenhum aviso se a verificação automática for desativada dessa forma. Entretanto, a Central de Segurança do Windows o alertará.

OBSERVAÇÃO: Desmarcar a caixa de seleção Ativar verificação automática significa que a verificação permanecerá desativada até que seja ativada manualmente novamente.

2. A partir da menu da bandeja do sistema clique em **Iniciar verificação automática**.
   - Essa opção alterna entre **Iniciar a verificação automática** e **Interromper a verificação automática**.
   - Se a verificação for interrompida manualmente, ela será ativada da próxima vez que o computador for reiniciado ou quando uma atualização do Security Suite for instalada.

Remover automaticamente os vírus detectados

O verificador detecta e repara todos os tipos de vírus. Sempre que possível, o arquivo infectado é reparado antes que o arquivo seja transferido para o aplicativo. O acesso ao arquivo infectado é negado se o reparo falhar. Observe que o arquivo é totalmente excluído se ele somente contiver malware.

Copyright © 1990-2010 Norman ASA

Modos de usuário

A seção modos de usuário é dividida em dois módulos 'Usuário local' e 'Serviços e usuários remotos'. Em circunstâncias normais, uma estação de trabalho é executada no modo **Usuário local**, enquanto um servidor é executado no modo **Usuários de serviços e remotos**. As configurações padrão fornecem proteção suficiente para a maioria das situações e recomenda-se não alterá-las a menos que você esteja completamente consciente das consequências.

Usuário local

- **Ler/Executar**
  - Instrui o Verificador automático a verificar arquivos antes de serem utilizados.
  - Exemplo: Quando um usuário clica duas vezes em um arquivo doc., a Verificação "mediante acesso" verifica o arquivo assim como o aplicativo que está sendo iniciado (neste exemplo, o MS Word).
- **Verificação na leitura e gravação**
  - Instrui a Verificação automática a verificar os arquivos que são abertos para edição, por exemplo, quando um usuário faz um download de um arquivo da Internet.
  - Se você selecionou a verificação na **Leitura/Execução**, será possível fazer o download e salvar um arquivo infectado no disco. Entretanto, a Verificação automática detectará o vírus quando você tentar abrir o arquivo.

Serviços e usuários remotos

Esse modo se aplica a qualquer sistema operacional XP/Vista/Windows 7 que executa logoff e a qualquer máquina que teoricamente pode agir como um servidor. As seleções feitas aqui tem a finalidade de verificar os arquivos antes que eles sejam utilizados e/ou quando novos arquivos são criados ou quando arquivos existentes são alterados. Em outras palavras, é selecionada uma estratégia para a verificação automática que tem efeito quando você salva os arquivos baixados da Internet, de servidores FTP, quando outro computador escreve arquivos para um compartilhamento de rede no computador etc.

- **Gravar**
  - Instrui a Verificação automática a verificar arquivos salvos no disco, por exemplo, quando um usuário salva um arquivo em um servidor. Nesse caso, a Verificação automática no servidor verificará o arquivo.
- **Verificação na leitura e gravação**
  - Esperamos que você não precise utilizar essa opção. Um caso em que essa opção é útil é se um servidor for infectado, como resultado de uma atualização perdida do verificador, por exemplo. A verificação em leitura e gravação em tal situação evitará a propagação posterior da infecção por toda a rede.

Usar o Norman Sandbox

O recurso Sandbox é usado para detectar vírus novos e desconhecidos. Selecione esta opção se desejar que o verificador procure por novas variantes do vírus. O Sandbox é particularmente ajustado para encontrar novos worms de e- mail de rede e de pessoa-a-pessoa e vírus de arquivo e também irá reagir as ameaças desconhecidas à segurança.

- **Desativado**
  - O recurso Área de Segurança é desativado.
- **Normal**
  - Nível de verificação recomendado. Com essa opção ativada, o Sandbox verifica todas as operações escritas para usuários locais e para usuários remoto/serviços.
- **Ampliado**
  - Em uma situação crítica é possível selecionar esse modo, por exemplo, se existir um foco de vírus no sistema e nenhuma detecção com base em assinatura estiver disponível por um período limitada. O Sandbox então verificará na leitura e na execução. Quando esta opção for selecionada, o tempo de verificação irá aumentar, mas não deve afetar consideravelmente o desempenho do sistema.

Clique em **Salvar** para confirmar as alterações.

Copyright © 1990-2010 Norman ASA

Verificador manual

Utilize a Verificação manual para verificar áreas selecionadas do computador. A verificação de todo o disco rígido é uma tarefa que exige muito tempo. Para verificações periódicas de unidades inteiras, pastas ou arquivos selecionados, recomenda-se verificações programadas. Utilize o Editor de Tarefas e ative a Verificação de proteção de tela de modo que as verificações manuais sejam executadas automaticamente durante períodos de pouca atividade ou de ociosidade. Por fim, você pode clicar com o botão direito do mouse em um objeto do sistema de arquivos para iniciar a Verificação manual. Todos esses métodos de verificação utilizam as configurações do Verificador manual.

Usar o Sandbox

O recurso Sandbox é usado para detectar vírus novos e desconhecidos. Selecione esta opção se desejar que o verificador procure por novas variantes do vírus. O Sandbox é particularmente ajustado para encontrar novos worms de e- mail de rede e de pessoa- a- pessoa e vírus de arquivo e também irá reagir as ameaças desconhecidas à segurança. Quando esta opção for selecionada, o tempo de verificação irá aumentar, mas não deve afetar consideravelmente o desempenho do sistema.

Remover automaticamente os vírus detectados

O aplicativo irá tentar remover o vírus do arquivo infectado Selecione esta opção para reparar automaticamente os arquivos infectados. A maioria dos vírus podem ser instantaneamente removidos, exceto os vírus do setor de boot. Um prompt para a intervenção do usuário sempre precede a remoção de um vírus do setor de boot. Observe que o arquivo é totalmente excluído se ele somente contiver malware.

Verificar arquivos

Selecione esta opção para incluir arquivos arquivados na verificação. Atualmente, há suporte para os seguintes formatos: ACE, APPLE_SINGLE, ARJ, BZIP2, CAB, GZ, LZH, MAIL, RAR, RAR3, SFXZIP, TAR, ZIP e 7Z.

Registrar

- **Cria um arquivo de registro**

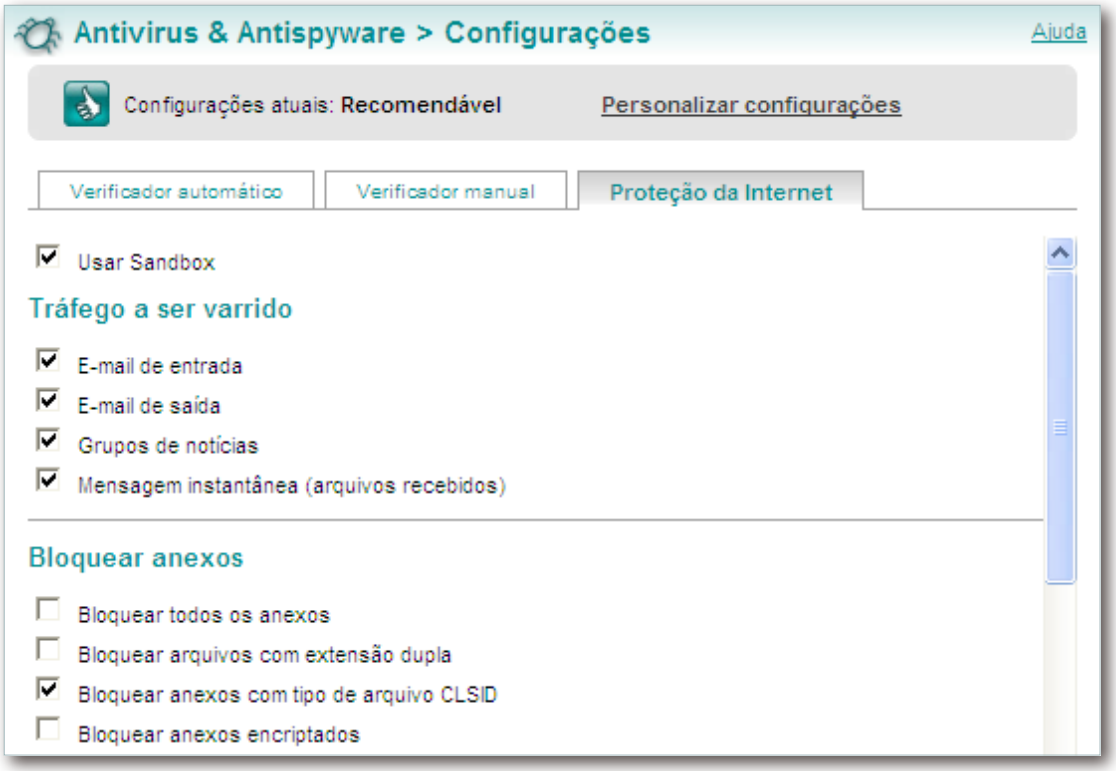
  Cria um arquivo de registro na pasta C:\Arquivos de Programas\Norman\Logs cada vez que uma verificação na demanda é executada. Se você cancela a seleção desta opção, nenhum arquivo de registro é criado nas verificações na demanda. Esta opção é ativada por padrão.

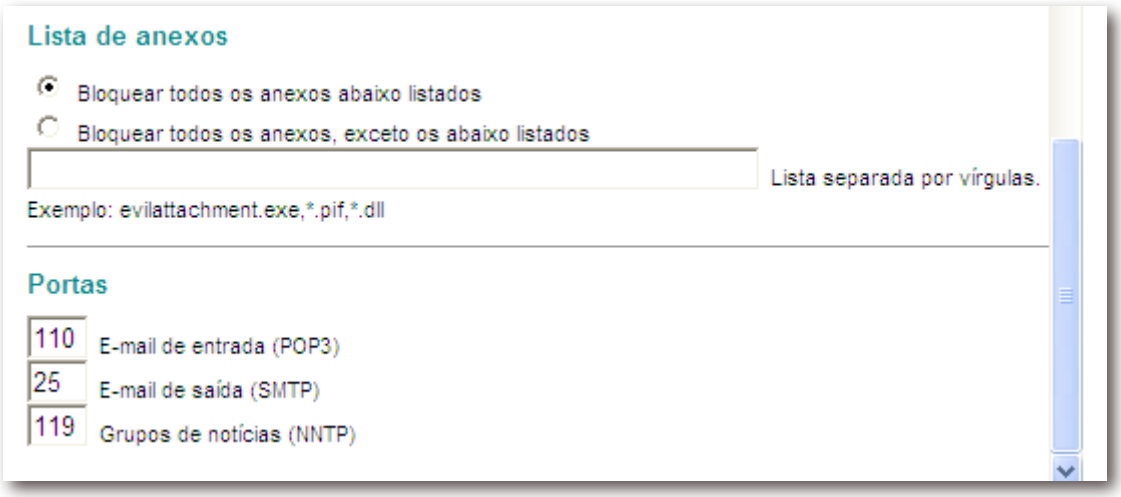
- **Registro detalhado**
  Gera um relatório detalhado, especificando cada arquivo que foi varrido, tempo de varredura por arquivo, status, etc.

Copyright © 1990-2010 Norman ASA

Proteção da internet

Esse é um filtro que protege contra a propagação de vírus por e-mails e news readers da Internet. A maioria dos vírus relatados hoje utilizam mecanismos que os capacitam a espalhar-se por e-mail. Esse módulo de filtro foi projetado para interceptar e-mails e notícias enviados e recebidos e para revelar ou bloquear todos os anexos infectados por conteúdo indesejável. É capaz de escanear vírus desconhecidos nos e-mails e de bloquear anexos de arquivo dependendo do conteúdo e das extensões do arquivo.





Usar o Sandbox

O recurso Sandbox é usado para detectar vírus novos e desconhecidos. Selecione esta opção se desejar que o verificador procure por novas variantes do vírus. O Sandbox é particularmente ajustado para encontrar novos worms de e- mail de rede e de pessoa-a-pessoa e vírus de arquivo e também irá reagir as ameaças desconhecidas à segurança. Quando esta opção for selecionada, o tempo de verificação irá aumentar, mas não deve afetar consideravelmente o desempenho do sistema. Para obter mais informações sobre o Sandbox, consulte “Apêndice A” na página 63.

Copyright © 1990-2010 Norman ASA

Tráfego a ser verificado

Selecione quais elementos do tráfego de Internet deseja verificar. O padrão é verificar tudo.

- **e-mail de entrada (POP3),**
  - Verifica todos os e-mails que você recebe de outros. Novamente, mesmo que seu melhor amigo ou seu associado comercial mas próximo não tenha conhecimento da infecção por vírus.
- **E-mail de saída (SMTP),**
  - Verifica todos os e-mails que são enviados de seu sistema. Se sua máquina estiver infectada por malware sobre o qual você não está ciente, poderia então enviar de forma não intencional e-mails infectados para amigos e associados comerciais, por exemplo.
- **Grupos de notícias (NNTP)**
  - Varre o tráfego gerado entre seu computador e outros participantes no grupo/fórum em que você está ativo.
- **Mensagem instantânea (arquivos recebidos),**
  - Varre o tráfego de transferência de arquivo durante as sessões de mensagens instantâneas com o MSN Messenger e o Window Messenger. Quando esta opção for selecionada, os arquivos de entrada são varridos para detectar malware. Se um arquivo está infectado uma mensagem suspensa irá alertar sobre o incidente
  - Somente arquivos transferidos são varridos, portanto, links infectados ainda apresentam uma ameaça.

Observe que os arquivos transferidos são varridos quando são gravados no diretório ...\Arquivos temporários da Internet**. Se malware for detectado, provavelmente é um arquivo .tmp em quarentena. Para restaurar um arquivo .tmp em quarentena, selecione o arquivo desejado, escolha a opção** Salvar como **no menu ao clicar com o botão direito do mouse, e salve o arquivo com seu nome e extensão originais. Consulte "Quarentena" na página 18.**

Bloquear anexos

Este recurso é particularmente útil quando worms de e-mail são do tipo roaming e o worm pode ser identificado pelo nome do arquivo. O bloqueio de anexo também é um recurso útil para parar tipos de arquivos que você não deseja receber em sua caixa de correio. Quando um anexo é bloqueado, ele é movido para a área de quarentena ao invés de ser excluído. Você pode bloquear anexos pelo nome ou extensão ao inserir as informações exatas. Essa uma explicação resumida das opções de configurações disponíveis:

- **Bloquear todos os anexos**
  - Todos os anexos são bloqueados.
- **Bloquear arquivos com extensão dupla**
  - muitos worms e vírus de e-mail aplicam um técnica segundo a qual se acrescenta uma extensão adicional. Por exemplo **Nome do arquivo.jpg.vbs**. A maioria dos clientes de e-mail ocultam a última extensão, para que o anexo pareça ter apenas a extensão .jpg. Entretanto, esse recurso não é apenas utilizado pelos vírus — arquivos autênticos com nomes semelhantes a **myfile.hlp.zip** e **todolist20.dec.doc** são ambos considerados como extensões duplas.
- **Bloquear anexos com tipo de arquivo CLSID**
  - Alguns worms e vírus recentes de e-mail aplicam a técnica CLSID para enganar os verificadores de e-mail e software de bloqueio. Eles tiram vantagem de um recursos do Windows que tornam possível substituir uma extensão .exe por uma extensão {...} e, portanto, evadir o bloqueio de arquivos .exe. Como não há motivo para que anexos legítimos usem este tipo de extensão, este comportamento é bloqueado por padrão.
- **Bloquear anexos encriptados**
  - Dependendo das ferramentas usadas, arquivos comprimidos e encriptados são geralmente mais difíceis de serem varridos para verificar a existência de vírus do que anexos de arquivos simples. Portanto, o aplicativo antivírus oferece a opção de bloquear todos estes anexos juntos.

Copyright © 1990-2010 Norman ASA

Lista de anexos

Use esta função para selecionar explicitamente os anexos que deseja bloquear ou certificar. Você pode inserir o nome exato do anexo ou usar cartões curinga (*) para bloquear determinadas extensões. A entrada aparece na caixa de listagem, onde é possível editá-la ou removê-la.

Por exemplo, digite `*.exe` para bloquear ou permitir todos os anexos com uma extensão .exe. Coloque o caractere curinga no começo e no fim do termo pesquisado. Não coloque o caractere curinga no meio do termo pesquisado.

- **Bloquear todos os anexos abaixo listados**
  - Todos os nomes que você **Adicionar** à lista são **BLOQUEADOS**.
  - Clique em **Salvar** para confirmar.
- **Bloquear todos os anexos exceto os abaixo listados**
  - Todos os nomes que você **Adicionar** à lista são **ACEITOS**.
  - Clique em **Salvar** para confirmar.

OBSERVAÇÃO: É muito importante que você diferencie cuidadosamente entre essas duas opções, pois elas representam dois extremos: BLOQUEAR todos na lista ou ACEITAR todos na lista.

Consulte o arquivo de ajuda do aplicativo para mais informações sobre esse assunto.

Remover entradas

Selecione uma ou mais entradas e clique em **Remover item(s) selecionado(s)**. Clique em **Salvar** para confirmar.

Portas

Entre os numerosos protocolos de comunicação entre computadores, há alguns que são fundamentais para utilizar a Internet. Por questões de padronização, os protocolos têm números de portas pré-atribuídos.

Números das portas

Alguns dos protocolos de comunicação entre computadores são vitais para o uso da Internet. Por questões de padronização, os protocolos têm números de portas pré-atribuídos. Na seção Tráfego a ser verificado foi selecionado qual tráfego de Internet você deseja verificar. Isso identifica os protocolos necessários para enviar e receber e-mail e o número da porta correspondente no computador, de acordo com o padrão da indústria.

Você pode ter atribuído diferentes números de portas para um ou mais dos protocolos aqui listados. Se este for o caso, é preciso inserir o número real da porta para o(s) protocolo(s) afetado(s).

Os protocolos abaixo são os que no momento são suportados. Esta lista será atualizada quando for necessário. Os números das portas e funções já estão especificados na caixa de diálogo:

- **E-mail de entrada (POP3)**
  (Porta 110) POP é uma abreviatura para Post Office Protocol.
- **E-mail de saída (SMTP)**
  (Port 25) SMTP é uma abreviatura para Simple Mail Transfer Protocol.
- **Grupos de notícias (NNTP)**
  (Port 119) NNTP é uma abreviatura para Network News Transfer Protocol.

Copyright © 1990-2010 Norman ASA

Outros métodos de verificação

Ativar o verificador da proteção de tela

Ao selecionar a Verificação de proteção de tela, uma verificação de vírus do sistema é executado durante períodos de ociosidade. O tempo de ociosidade é um período no qual não há atividade no sistema, ou seja, nenhuma tecla acionada ou nenhum movimento do mouse.

A verificação manual inicia um exame de todos os discos rígidos quando o protetor de tela é iniciado. Assim que o computador é ativado, por exemplo, pelo movimento do mouse ou por pressionar um tecla, a proteção de tela é finalizada. Se a varredura for interrompida antes da finalização, na próxima vez que for ativada, ela será interrompida onde foi ativada.

1. Acesse **Antivirus & Antispyware** e selecione **Ativar verificação de proteção de tela**.
   - O diálogo Propriedades de Exibição do Painel de Controle do Windows aparece.

2. Selecione **Norman Screensaver** da lista suspensa **Proteção de tela**.
   - Clique em **Pré-visualizar se desejar ver a proteção de tela** funcionando.
   - A pré-visualização é finalizada ao mover o mouse ou pressionar um tecla.
3. Clique em **OK** para confirmar as alterações.

Da próxima vez que o sistema estive ocioso e o Norman Screensaver estiver ativado, a verificação manual começará a verificar os discos rígidos, exibindo o progresso continuamente. A Verificação de proteção de tela será finalizada ao mover o mouse ou pressionar uma tecla.

OBSERVAÇÃO: Uma verificação de proteção de tela utiliza as mesmas configurações conforme especificado para a verificação manual.

Verificação com o botão direito do mouse

Essa é a verificação manual que inicia uma verificação do arquivo ou pasta selecionado por meio do menu suspenso do botão direito do mouse.

- Clique com o botão direito do mouse em um arquivo ou pasta.
  - Por exemplo, no Windows Explorer ou na área de trabalho.
- Selecione **Verificar vírus** do menu suspenso.
- O diálogo **Verificação manual** surgirá. Você pode **Navegar** para outro arquivo ou pasta para verificação e **Iniciar**, **Pausar** ou **Interromper** o processo de verificação.

Verificação pela linha de comando

A varredura pela linha de comando é uma alternativa à varredura com base na Interface Gráfica de Usuário (GUI) e oferece a possibilidade de executar trabalhos em segundo plano e outras tarefas de varredura a partir da linha de comando. A varredura pela linha de comando é uma boa alternativa para quem tem familiaridade com esse ambiente.

Copyright © 1990-2010 Norman ASA

A varredura pela linha de comando tem a mesma funcionalidade básica das varreduras a partir dos menus e não depende de nenhum outro módulo. Além disso, pode ser executada também a partir de arquivos de lote.

Iniciando a varredura pela linha de comando

1. Iniciando a varredura pela linha de comando
   - Acesse **Iniciar** > **Executar**.
   - Digite CMD e clique em **OK** ou pressione **Enter**.
2. Acesse o diretório onde o aplicativo Antivirus & Antispyware está instalado.
   - O local padrão é is `C:\Arquivos de Programas\Norman\nvc\bin\`
3. Digite os parâmetros desejados e pressione Enter.
   - Para obter uma lista de parâmetros disponíveis, digite
     ```
     nvcc /?
     ```
   - A sintaxe é:
     ```
     nvcc [unidade]:[caminho] [/parâmetros] [Enter]
     ```
   - Deve haver um espaço antes de cada parâmetro que você utilizar.

Copyright © 1990-2010 Norman ASA

Personal Firewall

Finalize o assistente de instalação (consulte “Assistente de Instalação” na página 12). Abra o aplicativo Security Suite e selecione **Personal Firewall** do menu do lado esquerdo. Consulte o “Guia de Introdução” na página 13 para obter instruções de como abrir o aplicativo e “Personal Firewall” na página 6 para obter uma descrição da finalidade e função do aplicativo. Consulte “Assistente de Instalação” na página 12 como inicializar o Personal Firewall.

Visualização principal

NORMAN SecuritySuite
Principal
Antivirus & Antispyware
Personal Firewall
Ferramentas de Perito
Configurações
Antispam
Parental Control
Privacy Tools
Intrusion Guard
Instalar e atualizar
Centro de suporte
Personal Firewall
Ajuda
Configurações atuais: Recomendável
Personalizar configurações
Bloqueado 0 conexões de entrada
Bloqueado 0 conexões de saída
Bloqueado 0 verificações de porta
Desativar Personal Firewall
O Personal Firewall está em execução.
Bloquear
Bloquear acesso à rede/Internet.
Limpar regras da sessão
Excluir regras temporárias de firewall desde a última reinicialização.
Excluir regras de bloqueio
Se um de seus aplicativos não puder acessar a Internet, é possível excluir todas as regras de bloqueio. Você será solicitado na próxima vez que tentar acessar a Internet.
Ferramentas de Perito
Utilitário de registro em tempo real e Visualizador de portas avançadas.

Este capítulo trata da configuração do aplicativo, criação de regras que controlam os aplicativos de entrada e saída, visualização de tráfego e muito mais. O aplicativo diferencia entre usuários inexperientes e experientes. Considerando que o usuário inexperiente é guiado por um assistente de instalação, o usuário experiente tem permissão para realizar a configuração detalhada das configurações avançadas.

Personalizar configurações

Clique nesta opção para editar os valores padrão. Consulte as “Configurações” do Personal Firewall na página 39. Para obter informações gerais sobre selecionar configurações recomendadas versus configurações personalizadas, consulte “Configurações do Security Suite” na página 15.

Estatísticas

As estatísticas exibem informações sobre conexões bloqueadas de entrada e de saída e verificações de portas.

- **No. de conexões de entrada bloqueadas**.
  Alguém tentou se conectar com sua máquina, mas foi bloqueado, possivelmente porque você não tem o software requerido instalado. Tais conexões dificilmente são de natureza maliciosa, mas provavelmente requerem solicitações legítimas do servidor.
- **No. de conexões de saída bloqueadas**.
  O número de conexões de saída que foram bloqueadas por uma ou mais regras. Se muitas conexões de saída estão bloqueadas, você deveria verificar se as regras relevantes estão corretas.

Copyright © 1990-2010 Norman ASA

- **No. de verificações de portas bloqueadas**.
  Mostra quantas tentativas sistemáticas foram feitas para varrer portas abertas. Algumas vezes os vírus podem varrer por portas abertas em uma tentativa de propagar, mas pode ser apenas uma ação legítima executada por software administrativo.

Desativar Personal Firewall (Ativar)

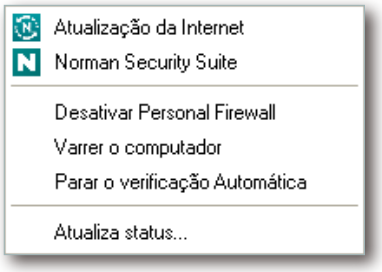
Clicar no link alterna entre ativar e desativar o Personal Firewall. É possível ativar ou desativar o Personal Firewall a partir da página principal do aplicativo ou do menu da bandeja do sistema .

- Acesse a página principal do Personal Firewall e selecione **Desativar Personal Firewall**.

OBSERVAÇÃO: A Central de Segurança do Windows também emite uma mensagem de advertência quando o firewall é desativado

ou

- Clique com o botão direito do mouse no ícone da bandeja do sistema e selecione **Desativar Personal Firewall**.



OBSERVAÇÃO: Essa opção não está disponível no Windows Vista, no qual você deve desativar e ativar o Personal Firewall no console.

Bloquear

Clicar no link alterna entre bloquear e desbloquear todo o acesso à rede, incluindo à Internet. Você pode desejar usar esta função se deixar o PC ligado quando está afastado dele.

Limpar regras da sessão

Selecione esta opção para excluir as regras temporárias do firewall criados desde a última reinicialização do computador. As regras temporárias do firewall são criadas durante uma sessão, ou seja, entre duas reinicializações do computador ao selecionar **aplica-se a esta sessão** a partir do diálogo suspenso do firewall. Esta diálogo aparece quando uma ação requer que você decida permitir ou negar. Uma ação é, por exemplo, quando um programa tenta se conectar à Internet. Você será solicitado a confirmar a remoção das regras.

Excluir regras de bloqueio

Se não for possível acessar a Internet/rede, possivelmente uma regra esteja bloqueando a conexão. Clique nessa opção para remover todas as regras de bloqueio. Você será avisado na próxima vez que tentar acessar a Internet.

Ferramentas de Perito

Consulte a próxima seção.

Copyright © 1990-2010 Norman ASA

Ferramentas de Perito

As ferramentas especializadas consistem no Editor de regras, no Utilitário de registro em tempo real, no Visualizador avançado de portas e no recurso de Exportar e importar regras do Personal Firewall. Com essas ferramentas é possível administrar os aspectos avançados desse aplicativo.

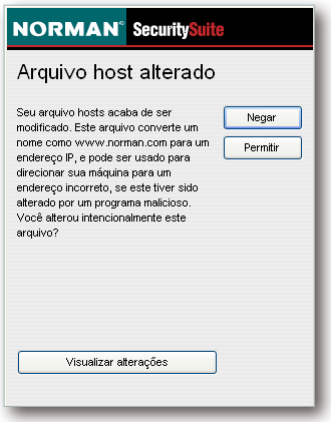
As ferramentas especializadas são destinadas a usuários experimentados. Exceto, naturalmente, a partir do modo do assistente do Editor de Regras, perfeito para usuários inexperientes. É possível alternar entre o modo de assistente e o modo avançado no diálogo do Editor de Regras.

É possível editar ou estabelecer regras utilizando o editor de regras. As regras do Firewall são necessárias para permitir o acesso de aplicativos confiáveis à Internet e bloquear conexões não confiáveis. O firewall emprega técnicas avançadas de sigilo que tornam seu computador invisível e indetectável na Internet. Você pode monitorar as atividades do computador utilizando o utilitário de registro em tempo real e o visualizador avançado de portas

Personal Firewall > Ferramentas de Perito
Ajuda
Editor de regras
Visualizar e modificar regras permanentes.
Utilitário de registro em tempo real-
Atividade da rede, detalhes de configuração.
Visualizador avançado de portas
Visualizar o status da porta e editar as regras correspondentes.
Exportar regras de Personal Firewall
Backup das regras e configurações de Personal Firewall.
Importar regras de Personal Firewall
Restaurar um backup das regras e configurações de Personal Firewall. Suas regras existentes serão substituídas.

Editor de regras

As regras são necessárias para permitir acesso à Internet por parte de aplicativos “confiáveis”, já que tantos programas contam com isso atualmente. As regras estabelecidas do Firewall para os programas de confiança instalados no computador quando você executou o assistente de instalação. Portanto, você pode ter programas instalados não reconhecidos ou que foram adquiridos depois que você instalou o firewall. Quando esse programa tenta se conectar à rede, o Personal Firewall gera uma janela pop-up que informa sobre a ação e deixa você decidir se permitirá ou negará a ação.


NORMAN SecuritySuite
Arquivo host alterado
Seu arquivo hosts acaba de ser modificado. Este arquivo converte um nome como www.norman.com para um endereço IP, e pode ser usado para direcionar sua máquina para um endereço incorreto, se este tiver sido alterado por um programa malicioso. Você alterou intencionalmente este arquivo?
Negar
Permitir
Visualizar alterações

Copyright © 1990-2010 Norman ASA

O Personal Firewall não permite criar regras de entrada. As regras de entrada são gerenciadas pela consciência do Modo de servidor do Personal Firewall, que cria dinâmica ou automaticamente as regras de entrada com base nos Privilégios do servidor. Esse é um mecanismo inteligente do firewall que avalia tentativas externas que merecem atenção em um conjunto de portas. As solicitações autênticas recebem acesso apenas para as portas relacionadas e são fechadas automaticamente quando não são mais necessárias.

Ao executar o Assistente de Instalação do Personal Firewall você seleciona entre usuário experiente e inexperiente. O Editor de Regras difere segundo o nível de usuário selecionado.

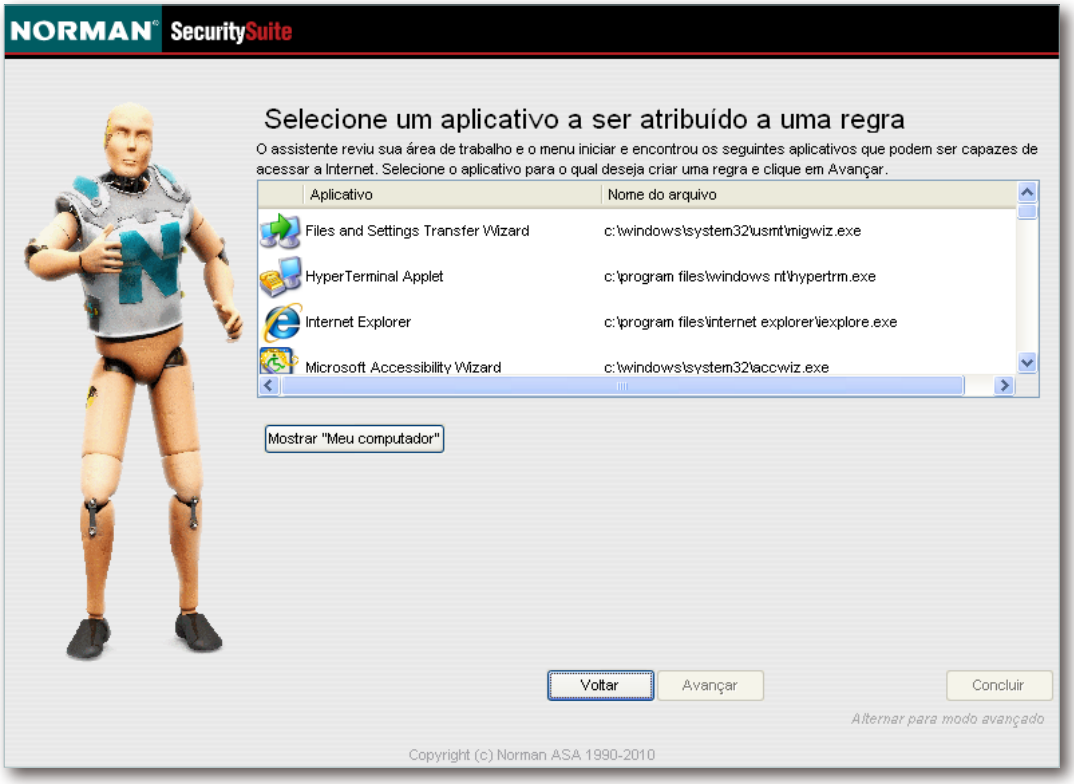
DICA

ALTERAR MODO DE USUÁRIO: No canto inferior direito do diálogo do Editor de Regras há uma opção para selecionar o modo de usuário. Essa opção alterna entre *Alterar para o modo de assistente* **e** *Alterar para o modo avançado*.

Nível inexperiente (Modo de assistente)

Acesse **Personal Firewall > Ferramentas Especializadas** e clique em **Editor de Regras** para abrir o diálogo do Assistente de Regras.

1. **Assistente de Regras**
   - Selecione **Desejo criar uma nova regra** e clique em **Avançar**.


NORMAN SecuritySuite
Selecione um aplicativo a ser atribuído a uma regra
O assistente reviu sua área de trabalho e o menu iniciar e encontrou os seguintes aplicativos que podem ser capazes de acessar a Internet. Selecione o aplicativo para o qual deseja criar uma regra e clique em Avançar.
Aplicativo
Nome do arquivo
Files and Settings Transfer Wizard
c:\windows\system32\usmt\migwiz.exe
HyperTerminal Applet
c:\program files\windows nt\hypertrm.exe
Internet Explorer
c:\program files\internet explorer\iexplore.exe
Microsoft Accessibility Wizard
c:\windows\system32\accwiz.exe
Mostrar "Meu computador"
Voltar
Avançar
Concluir
Alternar para modo avançado
Copyright (c) Norman ASA 1990-2010

2. **Selecione o aplicativo para atribuir uma regra.**
   - Uma lista de aplicativos qualificados é apresentada: Clique em um aplicativo para selecioná-lo. Selecione **Exibir Meu Computador** para navegar no computador e localizar programas que não estão na lista. Clique em **Avançar** para continuar.
3. **Ação para este aplicativo?**
   - Selecione **Permitir** ou **Negar** o acesso deste aplicativo à Internet. Clique em **Avançar** para continuar.

Copyright © 1990-2010 Norman ASA

4. **É um aplicativo de servidor?**
   - Determine se esse é ou não um aplicativo do servidor. Os aplicativos de servidor mantém as portas abertas e visíveis – fazendo com o que o computador se comporte como um servidor – permitindo a conexão com outros computadores. Selecione **Não** se estiver em dúvida. Clique em **Avançar** para continuar.

DICA

O firewall avisará posteriormente se o aplicativo estiver solicitado privilégios de servidor. Um regra sempre pode ser alterada depois.

5. **Resumo**
   - Aparecerá uma caixa de diálogo de resumo. Clique em **Finalizar** para gerar a regra.
   - A regra terá efeito imediatamente após ter sido gerada.

Nível experiente (Modo avançado)

Acesse **Personal Firewall > Ferramentas Especializadas** e, em seguida, clique em **Editor de Regras**. Aparece uma caixa de diálogo que relaciona as regras existentes e seu status:

1. Clique em **Criar nova** e, em seguida, preencha os campos necessários.
2. Clique em **OK** para confirmar.

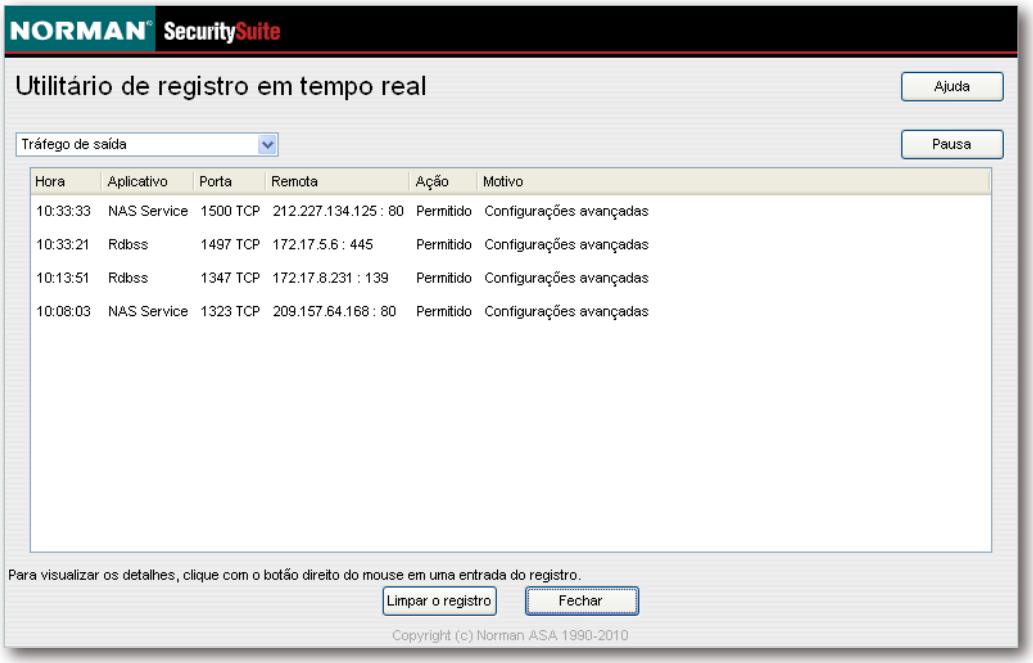
Para obter uma descrição detalhada de todos os campos, consulte os arquivos de ajuda do aplicativo.

Copyright © 1990-2010 Norman ASA

Utilitário de registro em tempo real

O Personal Firewall emprega técnicas avançadas de sigilo que tornam seu computador invisível e indetectável na Internet. É possível monitorar as atividades no próprio computador utilizando outros dois recursos: o **Utilitário de Registre em Tempo Real** e o **Visualizador Avançado de Portas**.

Acesse **Personal Firewall > Ferramentas Especializadas** e, em seguida, clique em **Utilitário de Registre em Tempo Real**. Clique com o botão direito do mouse para visualizar os detalhes e possivelmente alterar a configuração desse aplicativo.


NORMAN SecuritySuite
Utilitário de registro em tempo real
Ajuda
Tráfego de saída
Pausa
Hora Aplicativo Porta Remota Ação Motivo
10:33:33 NAS Service 1500 TCP 212.227.134.125 : 80 Permitido Configurações avançadas
10:33:21 Rdbss 1497 TCP 172.17.5.6 : 445 Permitido Configurações avançadas
10:13:51 Rdbss 1347 TCP 172.17.8.231 : 139 Permitido Configurações avançadas
10:08:03 NAS Service 1323 TCP 209.157.64.168 : 80 Permitido Configurações avançadas
Para visualizar os detalhes, clique com o botão direito do mouse em uma entrada do registro.
Limpar o registro
Fechar
Copyright (c) Norman ASA 1990-2010

Tráfego de saída

O registro especifica em que **Momento** um **Aplicativo** conectou-se à Internet, o nome do programa e de qual **Porta**, mencionando o endereço IP do computador **Remoto**, porta e **Ação**. A **Ação** é Permitida ou Negada. O **Motivo** é porque existe uma regra permanente ou uma regra de sessão para esta ação/aplicativo, se estiver definida na **Configuração avançada** ou na expiração de prompt de usuário.

Solicitações de privilégio ao servidor

O registro especifica em que **Momento** um **Aplicativo** conectou-se à Internet e em qual **Porta**, mencionando o endereço IP **Remoto** da máquina, porta e a **Ação** adotada pelo Firewall Pessoal. A **Ação** é Permitida ou Negada. O **Motivo** é porque existe uma regra permanente ou uma regra de sessão para esta ação/aplicativo, se estiver definida na **Configuração avançada** ou não há nenhum aplicativo obedecendo. O motivo mais comum para não permitir o tráfego de entrada, é porque sua máquina não tem o software requerido para interpretar a consulta. Em outras palavras; nenhuma coincidência de solicitação de privilégio de servidor.

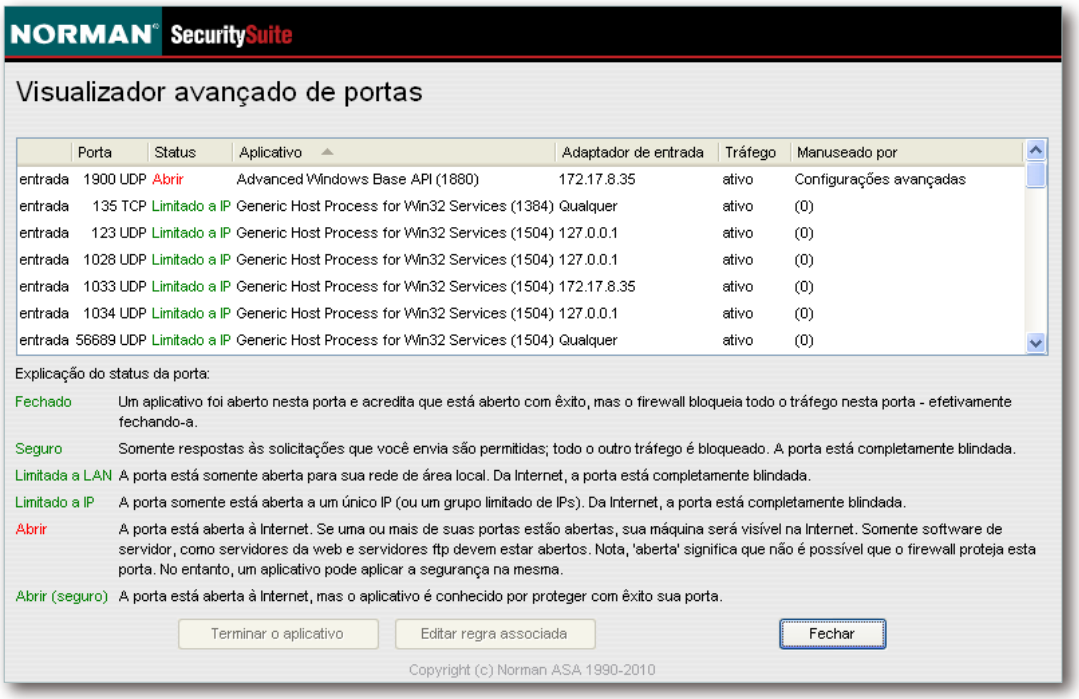
Para receber dados de outra máquina na rede, um aplicativo abre uma ou mais portas para obedecer. Observe que as solicitações de privilégio de servidor não são conexões estabelecidas, mas solicitações para conexões. No entanto, alguma vezes o aplicativo também abre uma porta para obedecer, para poder receber uma resposta de uma máquina para a qual envia dados. O Firewall Pessoal permite automaticamente tais respostas. Um mecanismo no Firewall Pessoal determina se um aplicativo abriu deliberadamente uma porta, ou se o aplicativo recebe uma solicitação espontânea, como se fosse um servidor. O Personal Firewall, então, solicita que o usuário confirme que ao aplicativo deveria ser concedido privilégios como um servidor.

Copyright © 1990-2010 Norman ASA

Visualizador avançado de portas

O Visualizador Avançado de Portas apresenta um panorama de todas as atividades nas portas atuais do computador. Você deve utilizar esse utilitário para verificar manualmente se algum malware infectou sua máquina.

Acesse **Personal Firewall > Ferramentas Especializadas > Visualizador Avançado de Portas**.


NORMAN SecuritySuite
Visualizador avançado de portas
Porta Status Aplicativo Adaptador de entrada Tráfego Manuseado por
entrada 1900 UDP Abrir Advanced Windows Base API (1880) 172.17.8.35 ativo Configurações avançadas
entrada 135 TCP Limitado a IP Generic Host Process for Win32 Services (1384) Qualquer ativo (0)
entrada 123 UDP Limitado a IP Generic Host Process for Win32 Services (1504) 127.0.0.1 ativo (0)
entrada 1028 UDP Limitado a IP Generic Host Process for Win32 Services (1504) 127.0.0.1 ativo (0)
entrada 1033 UDP Limitado a IP Generic Host Process for Win32 Services (1504) 172.17.8.35 ativo (0)
entrada 1034 UDP Limitado a IP Generic Host Process for Win32 Services (1504) 127.0.0.1 ativo (0)
entrada 56689 UDP Limitado a IP Generic Host Process for Win32 Services (1504) Qualquer ativo (0)
Explicação do status da porta:
Fechado Um aplicativo foi aberto nesta porta e acredita que está aberto com êxito, mas o firewall bloqueia todo o tráfego nesta porta - efetivamente fechando-a.
Seguro Somente respostas às solicitações que você envia são permitidas; todo o outro tráfego é bloqueado. A porta está completamente blindada.
Limitada a LAN A porta está somente aberta para sua rede de área local. Da Internet, a porta está completamente blindada.
Limitado a IP A porta somente está aberta a um único IP (ou um grupo limitado de IPs). Da Internet, a porta está completamente blindada.
Abrir A porta está aberta à Internet. Se uma ou mais de suas portas estão abertas, sua máquina será visível na Internet. Somente software de servidor, como servidores da web e servidores ftp devem estar abertos. Nota, 'aberta' significa que não é possível que o firewall proteja esta porta. No entanto, um aplicativo pode aplicar a segurança na mesma.
Abrir (seguro) A porta está aberta à Internet, mas o aplicativo é conhecido por proteger com êxito sua porta.
Terminar o aplicativo
Editar regra associada
Fechar
Copyright (c) Norman ASA 1990-2010

As portas abertas à Internet aparecem em vermelho e devem receber total atenção, como o Personal Firewall não pode proteger uma porta aberta. O software de servidor como FTP e servidores web tem um uso legítimo para portas abertas. Mas se um aplicativo desconhecido estiver ativo em uma porta aberta, há motivo para preocupação.

Interromper um aplicativo

Para interromper um aplicativo, realce uma entrada e clique em **Finalizar Aplicativo**. O aplicativo é finalizado imediatamente, mesmo quando aparecer na lista por aproximadamente um minuto.

Digitar uma Configuração Avançada de Abertura

Selecione uma entrada e selecione a opção **Abrir configurações avançadas**.

NORMAN SecuritySuite
Usar Network Time Protocol e permitir o tráfego através da porta 123
OK
Cancelar
Copyright (c) Norman ASA 1990-2010

OBSERVAÇÃO: Para alterar a configuração de um aplicativo de permitir para recusar, remova a marca de verificação e clique em OK. Como alternativa, marque a caixa de seleção para permitir que um aplicativo negado acesse a Internet. Observe que Finalizar aplicativo e Editar regra associada somente se aplica à entradas "administradas pela regra". A opção Abrir Configuração Avançada está disponível apenas para as regras controladas por 'configuração avançada'.

Copyright © 1990-2010 Norman ASA

Exportar regras do Personal Firewall

Faça backup das regras do Personal Firewall. Selecione **Exportar regras do Personal Firewall** e especifique o local. Salve o arquivo em uma mídia externa por motivos de segurança.

Importar regras do Personal Firewall

Restaure as regras do Personal Firewall. Selecione **Importar regras do Personal Firewall** e especifique a localização a partir de onde você deseja restaurar o arquivo de backup.

Copyright © 1990-2010 Norman ASA

Configurações

Configurar o Personal Firewall

Durante a instalação, diversas regras foram automaticamente criadas, incluindo regras para os navegadores mais comuns, clientes de correio, MSN e outros programas que precisam se conectar na rede.

Acesse **Personal Firewall > Configurações > Configurar Personal Firewall**. Para visualizar e/ou editar regras existentes, consulte “Editor de regras” na página 33.

Aplicativos de saída

Alguns aplicativos sem regras podem tentar conectar-se à Internet ou à rede de área local. Neste diálogo é possível decidir como o firewall pessoal deve controlar esses aplicativos. O configuração padrão **Perguntar**. Ao ser avisado você pode avaliar um aplicativo que tenta acessar a internet e definir uma regra, por exemplo. A alternativa é **Negar** em cujo caso todos os programas sem uma regra permanente ou com base na sessão têm o acesso negado à rede.

Privilégios do servidor

Alguns aplicativos sem regras podem tentar aceitar conexões da Internet. Neste diálogo é possível decidir como o firewall pessoal deve controlar esses aplicativos. O configuração padrão **Perguntar**. Ao ser avisado você pode avaliar se um aplicativo deve aceitar um convite de rede. A alternativa é **Negar** em cujo caso todos os programas sem uma regra permanente ou com base na sessão irão negar convites da rede.

OBSERVAÇÃO: Na caixa de diálogo Editar regra há uma opção que permite conceder ou negar privilégios de servidor para um aplicativo. O conceito privilégios de servidor também é explicado no tópico Editar regra**.**

Configurações avançadas

A natureza técnica destas opções de configuração requer um determinado conhecimento se você pretende alterar configurações padrão. Em princípio, não altere configurações, a menos que saiba o que significam e esteja ciente das consequências. As configurações-padrão são suficientes para o usuário médio.

A opção de Operação do Personal Firewall é descrita abaixo. Para obter mais detalhes de todas as opções, consulte os arquivos de ajuda do aplicativo.

Alterar modo de usuário (inexperiente/experiente)

Acesse **Personal Firewall > Configurações > Configuração avançada** e, em seguida, desloque até a seção **Operação do Personal Firewall.**

Esta opção está ativada se você especificou "Usuário experiente" durante a configuração. Se você especificou "Usuário inexperiente" irá iniciar em seu lugar o assistente de regras. A diferença entre esses dois níveis de usuário é o nível de assistência que você recebe ao criar novas regras ou alterar as regras existentes. Consulte “Editor de regras” na página 33 para obter mais informações sobre como criar regras em dois modos diferentes.

Copyright © 1990-2010 Norman ASA

Antispam

Abra o aplicativo Security Suite e selecione **Antispam** do menu do lado esquerdo. Consulte o “Guia de Introdução” na página 13 para obter instruções de como abrir o aplicativo e para 7 uma descrição da finalidade e função do aplicativo.

Visualização principal

Esse aplicativo oferece proteção contra e-mails comerciais não solicitados e em massa (spam) que podem conter ameaças para seu sistema. Este capítulo trata de personalizar o filtro de spam, criar listas de bloqueio e permissão, gerenciar e-mails filtrados, visualizar e-mails filtrados, atualizar intervalos e opções de gerenciamento de spam.

Estatísticas de spam

A visualização gráfica exibem o total de spams capturados e tentativas de phishing que o aplicativo bloqueou por dia nas últimas duas semanas.

Personalizar configurações

Clique nesta opção para editar os valores padrão. Consulte a seção “Configurações” de Antispam na página 43. Para obter informações gerais sobre selecionar configurações recomendadas versus configurações personalizadas, consulte “Configurações do Security Suite” na página 15.

Bloquear/Permitir

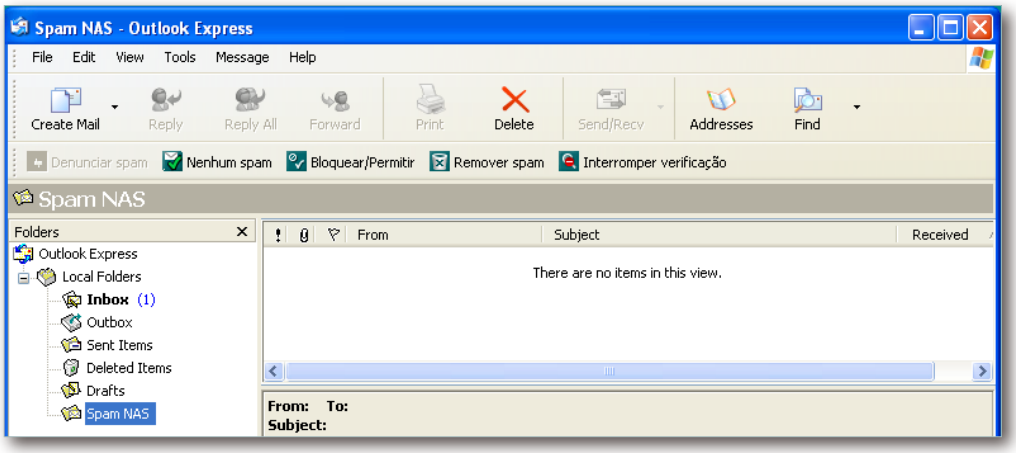
É possível gerenciar endereços de e-mails individuais utilizando a Lista de Bloqueio/Permissão para informar o aplicativo sobre endereços que sempre devem permitidos ou negados. O método de filtragem antispam jamais rejeitará a especificação manual de um endereço (Bloquear ou Permitir). Consulte a seção “Bloquear/Permitir” na página 42.

Copyright © 1990-2010 Norman ASA

Visualizar mensagens de e-mail filtradas

A partir do aplicativo de e-mail, por exemplo, Microsoft Outlook, Outlook Express ou Windows Mail, é possível visualizar as mensagens de e-mail filtradas como spam. A pasta Spam do NAS é criada ao instalar o Conjunto de Segurança Norman ou ao instalar um dos clientes de e-mail mencionados e o Norman Security Suite já estiver instalado no computador.

Abra o cliente de e-mail de sua preferência e localize a pasta Spam do NAS e o menu do aplicativo Antispam.



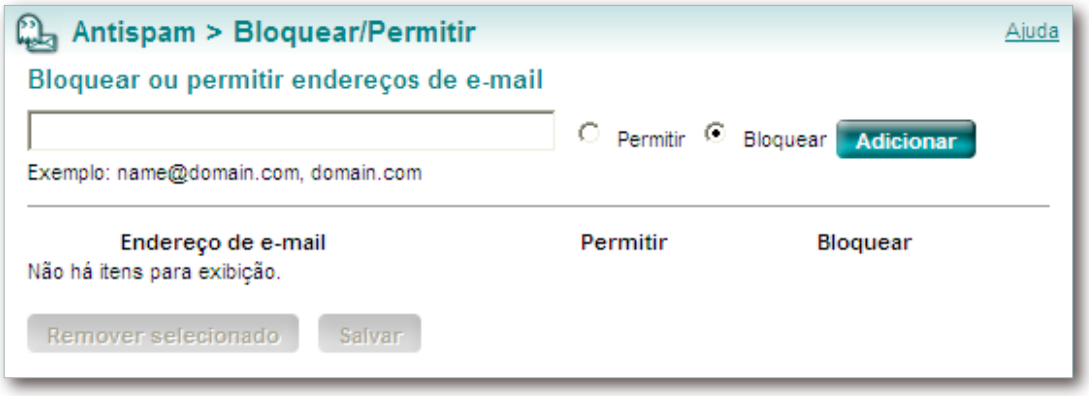
- **Denunciar Spam**
  - Denuncia e-mails como spam. Selecione uma mensagem de e-mail da Caixa de entrada e clique em **Denunciar Spam** a partir da barra de ferramentas. A mensagem é movida para a pasta **Spam do NAS**.
- **Não é Spam**
  - Marcar e-mails que não são spam. Selecione um ou mais e-mails da pasta **Spam do NAS** e clique em **Não é Spam**.
- **Bloquear/Permitir**
  - Bloqueia ou permite e-mails. Selecionar essa opção abre o aplicativo Norman Antispam. Digite um ou mais endereços de e-mail para **Bloquear** ou **Permitir**.
- **Remover Spam**
  - Apague o conteúdo preenchido da pasta **Spam do NAS**. Para excluir uma mensagem por vez clique com o botão direito do mouse em uma entrada e selecione **Excluir** do menu suspenso.
- **Verificar pasta**
  - Verifica se os e-mails recebidos são spams. Selecione uma ou mais pastas e clique em Verificar pasta para iniciar uma verificação manual. Essa opção alterna entre **Verifica pasta** e **Interromper verificação**. Clique em **Interromper verificação** para interromper a verificação das mensagens de spam.

Consulte “Controle de spam” na página 43 para especificar se deseja excluir o spam automaticamente.

Copyright © 1990-2010 Norman ASA

Bloquear/Permitir

É possível digitar manualmente o endereço de e-mail que você deseja bloquear ou permitir. Especifique se um endereço de e-mail deve ser bloqueado ou permitido selecionando o botão de seleção relevante.



Adicionar/remover endereço de e-mail

O endereço de e-mail que você digitar nesta caixa de diálogo aparecerá em uma lista. Ao digitar um novo endereço, a opção padrão **Bloquear** é para evitar o risco de permitir acidentalmente um endereço que você deseja bloquear. Como alternativa, selecione **Permitir** para aceitar e-mails desse remetente. É possível a qualquer momento editar os detalhes na lista de endereços de e-mail.

Adicionar

1. Digite um endereço de e-mail, por exemplo

   `nome1@domínio.com`
   ou
   - Digite vários endereços de e-mail separados por vírgula, por exemplo

     `nome1@domínio.com, nome2@domínio.com`
     ou
   - Digite um domínio inteiro para permitir ou bloquear, por exemplo

     `phoneysales.com`
   - Observação: Não adicione seu próprio domínio para evitar que os e-mails sejam falsificados.
2. Selecione **Permitir** ou **Bloquear** (Opção padrão) para cada endereço.
3. Clique em **Adicionar** para cada nova entrada.
4. Clique em **Salvar** para manter novos endereços ou domínios.

Remover

1. Selecionar um ou mais endereços.
2. Clique em **Remover item(s) selecionado(s)**.
3. Clique em **Salvar** para confirmar as alterações.

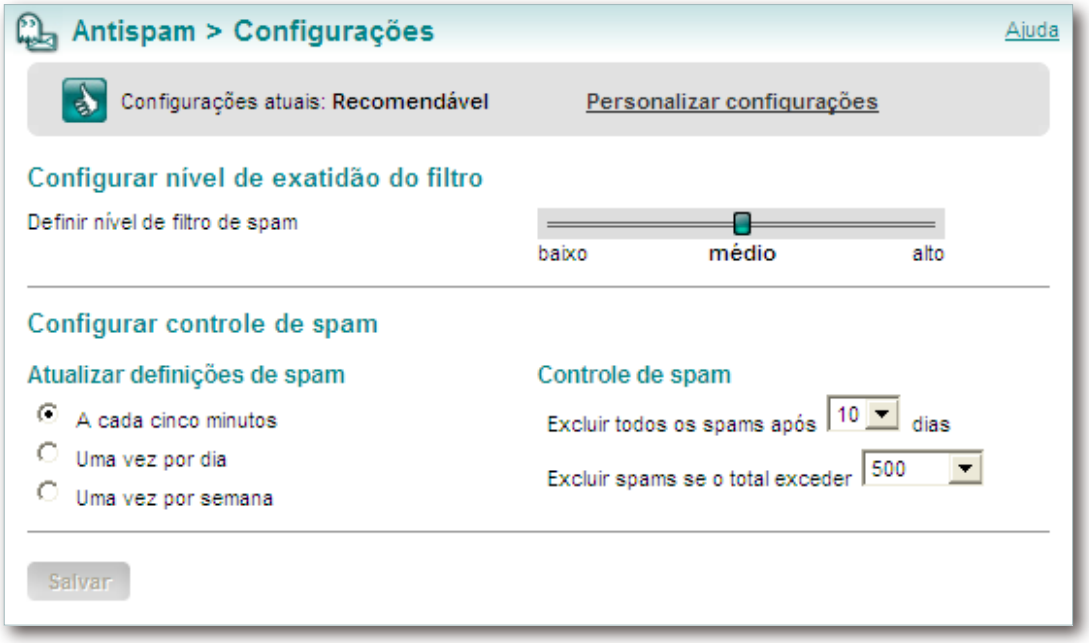
Editar

1. Selecionar um ou mais endereços.
2. Digite as alterações desejadas para o endereço de e-mail ou para bloquear/permitir.
3. Clique em **Salvar** para confirmar as alterações.

Copyright © 1990-2010 Norman ASA

Configurações

Tal como os aplicativos antivírus empregam arquivos de definição de vírus para detectar malwares, as soluções antispam utilizam arquivos de definição para filtrar e-mails não solicitados. Enquanto os arquivos de definição de vírus incorporam assinaturas de vírus que determinam se o arquivo está ou não infectado, as definições antispam utilizam um conjunto de critérios para calcular a probabilidade de um e-mail ser um spam. As definições de spam baseiam a análise de um e-mail no idioma, imagens, cores e links incluídos no e-mail, bem como o e-mail e o endereço IP do remetente. Mesmo assim, nem sempre é possível concluir com absoluta certeza se um e-mail é ou não um spam.



Configurar nível de rigor do filtro

Se você utilizar o controle deslizante e ajustar o nível de rigor para **Baixo**, o aplicativo Antispam examinará e-mails com máxima "suspeita" e consequentemente identificará menos e-mails como spam. Semelhantemente, se o controle deslizante for posicionado em **Alto**, uma interpretação mais ampla dos critérios de spam resultarão em uma pontuação mais baixa de spam para e-mails a serem identificados.

Quando há pouca ou nenhuma dúvida de que um e-mail é spam, por exemplo, quando o remetente está na lista negra ou em um banco de dados on-line, o e-mail será interrompido independente da posição da barra do controle deslizante. Consideramos a configuração padrão **Médio** como apropriada para filtrar e-mails indesejáveis.

O método de filtragem antispam jamais rejeitará a especificação manual de um endereço.

Configurar controle de spam

Atualizar definições de spam

Selecione a frequência para a atualização de definição de spam; a cada cinco minutos, uma vez um dia ou uma vez por semana. O valor padrão é atualizar os arquivos de definição a **Cada cinco minutos**.

Controle de spam

Essa opção permite fazer seleções ao excluir e-mails que o filtro de spam interrompeu, dependendo da época e quantidade. As configurações padrão são **Excluir todos os spams após** [10] **dias** e **Excluir spams se o total exceder** [500] mensagens de e-mail filtrados.

Lembre-se de clicar **Salvar** para confirmar qualquer alteração.

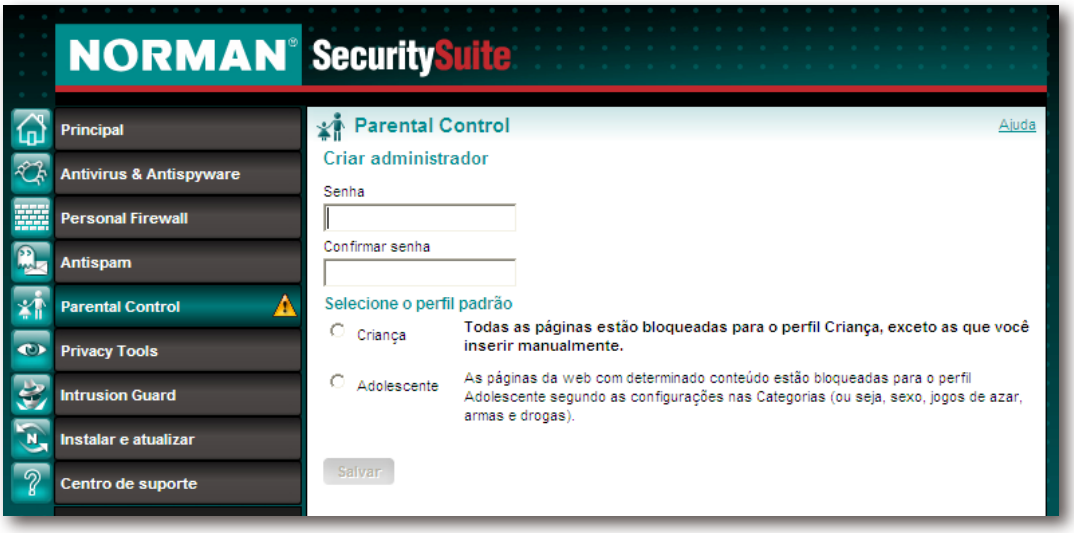
Copyright © 1990-2010 Norman ASA

Parental Control

Abra o aplicativo Security Suite e selecione **Parental Control** do menu do lado esquerdo. Consulte o “Guia de Introdução” na página 13 para obter instruções de como abrir o aplicativo e para 7 uma descrição da finalidade e função do aplicativo.

Acesso inicial

Antes de utilizar esse aplicativo pela primeira vez uma mensagem com as informações “*Administrador não criado*” aparecerá no painel Principal e um triângulo amarelo de aviso aparecerá no menu de entrada do aplicativo.



1. **Administrador não criado**

Você deve criar um perfil de administrador antes de acessar a esta aplicação. Digite uma senha e selecione o perfil de segurança padrão. Clique em **Salvar** para continuar.

O perfil de segurança padrão deve ser o perfil de usuário com a classificação mais inferior que você deseja criar. Ou seja, se você vai criar um perfil Criança, então, o perfil de segurança padrão deve também ser Criança. Somente o administrador pode editar usuários e configurar suas opções como programar o horário de acesso à Internet e criar listas de bloqueio e permissão. O administrador seria normalmente um pai.

Essas configurações podem ser alteradas depois a partir de **Parental Control > Configurações.**

OBSERVAÇÃO: A senha do administrador não pode ser redefinida. Certifique-se de selecionar uma senha que possa ser lembrada facilmente. A senha é sensível a maiúsculas e minúsculas.

2. **Login de administrador**

Quando um usuário administrador é criado a página de login aparece. Efetue login com o nome e senha do usuário administrador para acessar o aplicativo.

Ícone da bandeja do sistema

Um ícone da bandeja do sistema indica que o Parental Control está instalado. Mova o cursor do mouse sobre o ícone exibe um texto de status, por exemplo, ‘Parental Control: O ‘Administrador’ efetuou login’.

Copyright © 1990-2010 Norman ASA

Visualização principal

Este aplicativo bloqueia o acesso de determinadas categorias de websites e restringe e programa o acesso à Internet para os usuários. Este capítulo trata da criação, configuração e gerenciamento de usuários, assim como da visualização do registro e da programação do acesso à Internet. Efetue login com o nome e senha do usuário administrador para acessar o aplicativo.

Configurações

Clique nesta opção para editar os valores padrão. Consulte as “Configurações” do Parental Control na página 50.

Estatísticas

Da página principal é possível acompanhar as estatísticas no elementos bloqueados e verificados.

Configuração do usuário

Consulte a seção “Configuração do usuário” na página 46.

Visualizador do registro

Consulte a seção “Visualizador do registro” na página 50.

Copyright © 1990-2010 Norman ASA

Configuração do usuário

Criar usuários e atribuir perfis de usuário. Os usuários existentes estão listados neste diálogo com o nome de usuário e o perfil que lhes foram atribuídos.

Há três perfis de usuário, **Adulto**, **Adolescente** e **Criança**. O último é completamente restritivo e só permite o acesso a websites inseridos manualmente pelo administrador da lista de permissões.

Adulto	Nenhuma restrição.
Adolescente	Restrição de filtro de categorias.
Criança	Completamente restrito.

Categorias

As categorias têm base em uma ampla faixa de termos e expressões que permitem ao aplicativo identificar uma página da web como predominantemente orientado ao sexo, por exemplo. Os termos não são acessíveis para visualização ou edição. Para o perfil Adolescente, há quatro categorias disponíveis que irão bloquear o acesso às páginas da web com conteúdo do tipo **sexo**, **jogatina** , **armas** e **drogas**. Todas as categorias são por padrão ativadas, mas o administrador pode desmarcar as que deveriam ser permitidas.

Lista de bloqueio/Permissão

Para usuários do grupo Criança, deve haver uma lista de permissão, pois somente será possível visualizar os endereços que estiverem nessa lista. Para os usuários de perfil Adolescente é opcional criar uma lista de bloqueio e uma lista de permissões. Consulte as seções “Perfil Criança padrão” na página 47 e “Perfil Adolescente padrão” na página 47.

Formato do endereço web

URL (Uniform Resource Locator) é um termo técnico para um endereço web. Não há suporte para os caracteres curinga (*/?) nos endereços web. Os formatos válidos são:

- http://www.newspaper.com
- www.newspaper.com
- newspaper.com

Um dado endereço web permite que você acesse os níveis de subdomínio, mas nunca visitar um nível de pais. Por exemplo, a permissão de acesso ao site www.newspaper.com/kidsstuff não permite o acesso ao ao site www.newspaper.com de nível administrado pelos pais. Entretanto, se o site newspaper.com for adicionado, todos os subdomínios deste endereço da web são permitidos, como news.newspaper.com, cartoon.newspaper.com etc.

OBSERVAÇÃO: Se um usuário segue um link de uma página permitida, ele tem a permissão à despeito de para onde o link está conduzindo. No entanto, não é possível abrir outra página, a não ser que a referenciadora seja explicitamente permitida.

Copyright © 1990-2010 Norman ASA

Configurações padrão de perfil

O perfil **Adulto** não tem restrições. Os perfis **Criança** e **Adolescente** estão sujeitos a restrições e, dessa forma, podem ser configurados. Na verdade, se de qualquer forma um usuário designado para o perfil **Criança** precisa acessar a Internet, uma página da web deve ser especificada. As configurações de perfil aplicam-se a todos os membros do perfil de usuário. Para configurar um membro separado, consulte “Criar usuário” na página 48.

Perfil Criança padrão

Lembre-se de que as alterações efetuadas na lista de permissão afetam todo o perfil, não somente o usuário individual. Como todas as páginas da web para o perfil Criança estão bloqueadas, a não ser que estejam explicitamente permitidas, não há uma Lista de bloqueio ou Categoria para este perfil de usuário.

Adicionar

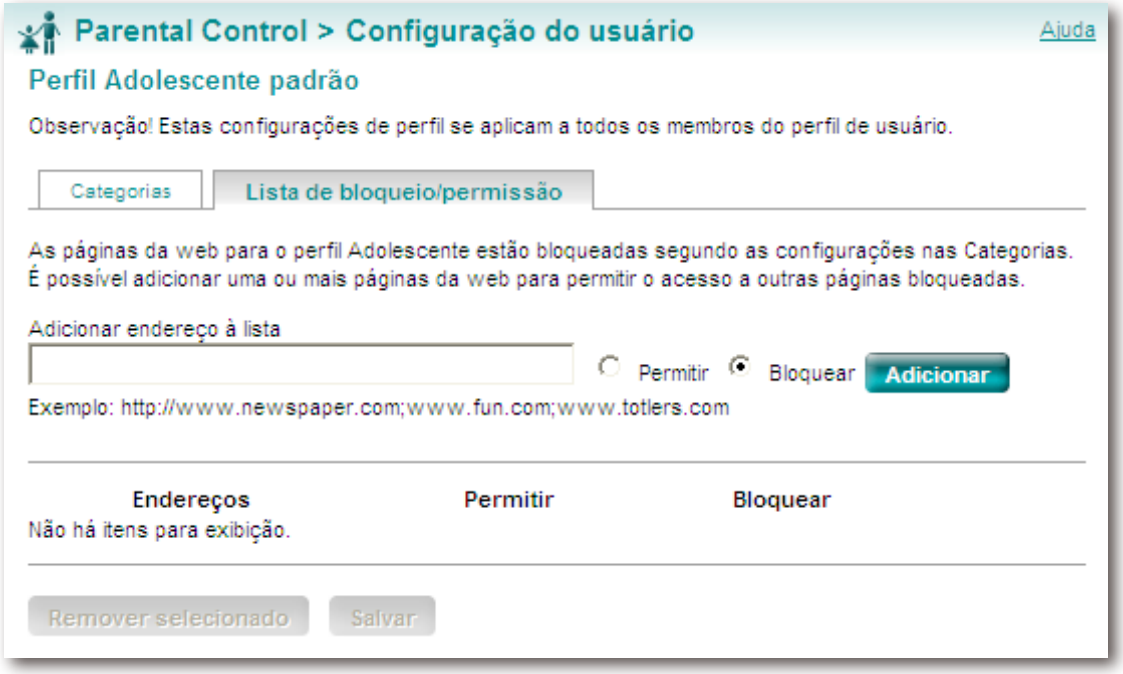
1. Digite um endereço web para permissão no campo **Adicionar endereço à lista**.
   - Digite vários endereços web separados por vírgula.
2. Clique em **Adicionar** para cada nova entrada.

Remover

1. Selecionar um ou mais endereços.
2. Clique em **Remover item(s) selecionado(s)**.

Perfil Adolescente padrão

Lembre-se de que as alterações efetuadas na lista de permissão afetam todo o perfil, não somente o usuário individual. Para este perfil as páginas da web são limitadas por Categorias e da lista de Bloqueio/Permissão.


Parental Control > Configuração do usuário
Ajuda
Perfil Adolescente padrão
Observação! Estas configurações de perfil se aplicam a todos os membros do perfil de usuário.
Categorias
Lista de bloqueio/permissão
As páginas da web para o perfil Adolescente estão bloqueadas segundo as configurações nas Categorias.
É possível adicionar uma ou mais páginas da web para permitir o acesso a outras páginas bloqueadas.
Adicionar endereço à lista
Permitir
Bloquear
Adicionar
Exemplo: http://www.newspaper.com;www.fun.com;www.totlers.com
Endereços
Permitir
Bloquear
Não há itens para exibição.
Remover selecionado
Salvar

Categorias

Por padrão, todas as categorias são selecionadas, ou seja, páginas da web com um determinado conteúdo são bloqueadas para o perfil Adolescente segundo essas configurações. As categorias são Sexo, Jogos, Armas e Drogas. O administrador pode remover a marca de seleção para permitir que páginas da web nessa categoria. Como alternativa, adicione uma ou mais páginas web à lista de Permissão. Clique em **Salvar** para confirmar as alterações.

Copyright © 1990-2010 Norman ASA

Lista de bloqueio/Permissão

Páginas da web para o perfil Adolescente são bloqueadas segundo as configurações nas Categorias. Você pode adicionar uma ou mais páginas da web para acessar, de outra maneira, páginas bloqueadas.

Adicionar

1. Digite um endereço web para permissão no campo **Adicionar endereço à lista**.
   - Digite vários endereços web separados por vírgula.
2. Clique em **Adicionar** para cada nova entrada.
3. Selecione o botão de seleção **Bloquear** ou **Permitir**.
4. Clique em **Adicionar** para cada nova entrada.

Criar usuário

Selecione **Criar usuário** a partir de **Controle de Pais > Configuração de usuário**.

1. Digite um nome para o novo usuário e, em seguida, digite uma senha que deverá confirmar.
2. **Selecione o perfil padrão** para basear o novo usuário.
   - Ao atribuir um perfil a um usuário, você determina que tipo de páginas da web o usuário pode visitar.
     - Adulto
       Nenhuma restrição. O usuário pode acessar qualquer website.
     - Adolescente
       Em princípio nenhuma restrição. Entretanto, as configurações padrão da Categorias bloqueará páginas da web com temas ou conteúdo indesejados.
     - Criança
       Autorizado a visualizar somente os tipos de páginas que o administrador inserir na Lista de permissão.
3. Clique em **Salvar** para confirmar.
   - Antes de clicar em **Salvar** para criar o novo usuário, você deve verificar se o perfil selecionado está correto para o usuário nomeado.

O novo usuário é adicionado à lista de usuários. Clique em um nome de usuário para configurar esse usuário.

Alterar senha

Altere o nome da conta e a senha para o usuário selecionado.

Categorias

Esta seleção só se aplica ao perfil de usuário Adolescente. Para permitir uma ou mais categorias para um usuário de perfil Adolescente, desmarque as caixas de seleção de categorias relevantes. Para obter mais informações, consulte a seção “Categorias” na página 46 e “Perfil Adolescente padrão” na página 47.

Lista de bloqueio/Permissão

Esta seleção só se aplica ao perfil de usuário Adolescente. A partir daqui, você pode permitir ou bloquear endereços da web para o usuário. Para obter mais informações, consulte a seção “Lista de bloqueio/Permissão” na página 46 e “Perfil Adolescente padrão” na página 47.

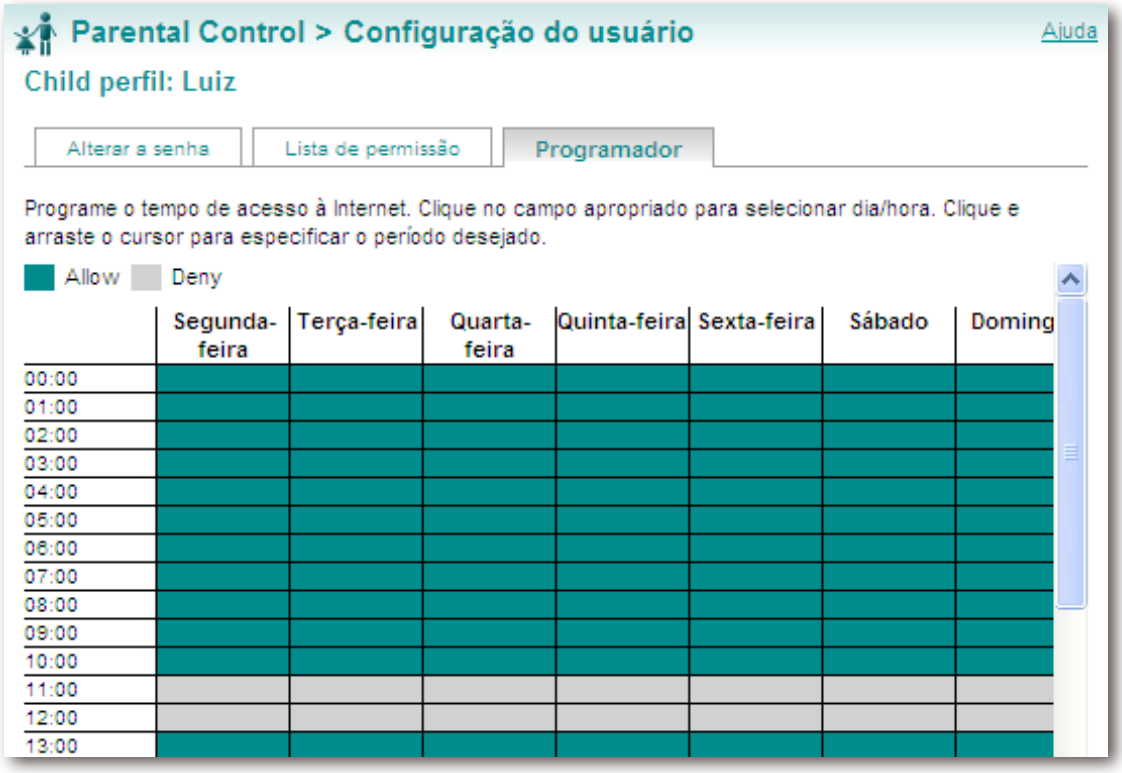
Lista de permissão

Esta seleção só se aplica ao perfil de usuário Criança. A partir daqui, você pode permitir ou bloquear endereços da web para o usuário. Consulte a seção “Perfil Criança padrão” na página 47.

Programador

O administrador pode decidir em que hora do dia, para cada dia da semana, que o usuário pode navegar na Internet. A configuração padrão é que todos os períodos são permitidos (Verde).

Copyright © 1990-2010 Norman ASA



1. Para bloquear o acesso à Internet por um período específico, coloque o cursor no período desejado e clique nele.
2. Clique e arraste o cursor para cima/para baixo ou para a direita/esquerda em movimento contínuo para estender o período que deseja bloquear. Do mesmo modo, clique e solte para mudar de **Negar** (cinza) para **Permitir** (verde).
3. Clique em **Salvar** para confirmar as alterações.

Copyright © 1990-2010 Norman ASA

Visualizador do registro

O aplicativo registra automaticamente as páginas da web bloqueadas para os usuários de perfil Adolescente e Criança. Os registros não mostram quais páginas o usuário visitou.

O registro pode mostrar as páginas bloqueadas por até uma semana. Existe um registro por dia na semana, e você somente pode selecionar um dia da semana, não uma data. O aplicativo sugere o dia atual da semana como o padrão.

As colunas no registro mostram a data, hora, usuário, motivo do bloqueio e o URL bloqueado.

Se a coluna Usuário estiver em branco, o sistema estava no modo de segurança sem um usuário conectado.

Configurações

Você pode evitar uma máquina automática com um usuário conectado com o usuário adulto que está sendo acessado por um usuário da criança (ou seja, se você esquecer de fazer logoff ou precisa deixar o computador de repente). O perfil padrão de segurança será ativado após o período especificado de inatividade.

Tempo ocioso antes de mudar para o perfil padrão

O tempo de ociosidade é um período no qual não há atividade no sistema, ou seja, nenhuma tecla acionada ou nenhum movimento do mouse.

- A partir do menu suspenso, selecione quando o Controle de Pais deverá ir para o perfil padrão quando o PC estiver ocioso.
- Clique em **Salvar** para confirmar.

Definir o perfil de segurança padrão

Você poderá selecionar Criança ou Adolescente como o usuário pois o aplicativo deve ser ativado após o período ocioso ser especificado.

- **Criança**
  Todas as páginas da web são bloqueadas para o perfil Criança, exceto as inseridas manualmente. Isso significa que até que você tenha adicionado uma página da web ao usuário Criança, nenhum acesso à Internet fica disponível.
- **Adolescente**
  Páginas da web com determinado conteúdo são bloqueadas para o perfil Adolescente segundo as configurações nas Categorias (ou seja, Sexo, Jogos, Armas e Drogas).
- Clique em **Salvar** para confirmar.

Alterar a senha do administrador

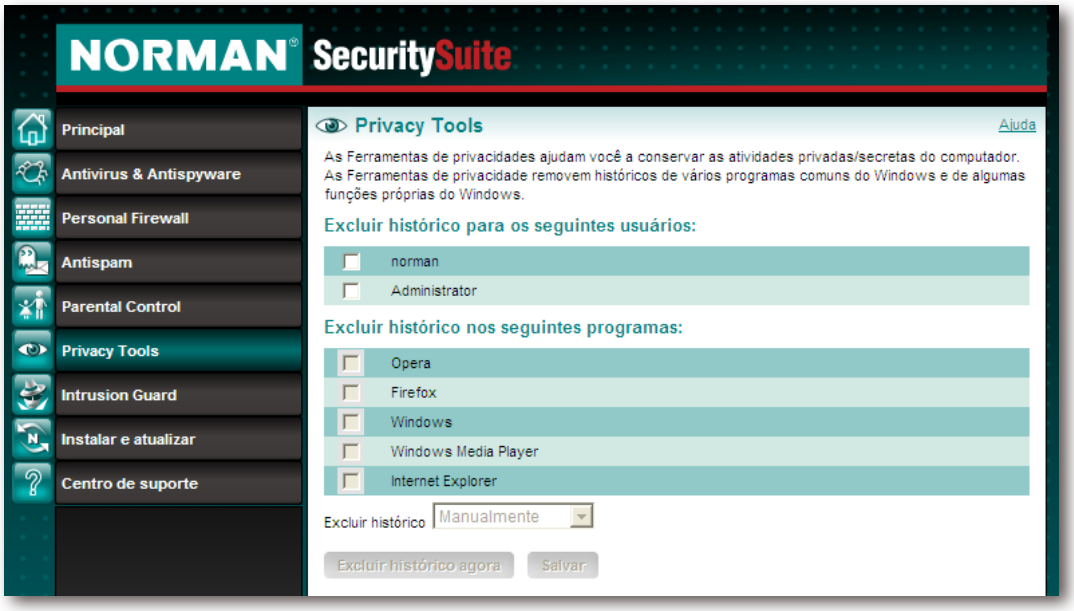
A senha de administrador não pode ser redefinida, mas você poderá mudá-la desde que saiba a antiga. Se você alterar a senha de administrador, poderá desejar anotá-la e mantê-la em um lugar seguro.

OBSERVAÇÃO: Observe que a senha é sensível a maiúsculas e minúsculas.

Copyright © 1990-2010 Norman ASA

Ferramentas de Privacidade

Abra o aplicativo Conjunto de Segurança e selecione **Ferramentas de Privacidade** do menu do lado esquerdo. Consulte o “Guia de Introdução” na página 13 para obter instruções de como abrir o aplicativo e o “Privacy Tools” na página 7 para obter uma descrição da finalidade e função do aplicativo.



Com este aplicativo é possível executar a exclusão segura de arquivos específicos. O conteúdo dos arquivos são permanentemente apagados e não pode ser recuperado. É possível também configurar o aplicativo para excluir automaticamente vários arquivos de registros contendo dados pessoais, cookies e histórico do navegador. A exclusão de registros do histórico não afeta as configurações e indicadores do aplicativo.

Excluir um histórico de programa do usuário

A lista de nome de usuários exibe todos os usuários registrados no computador e a lista de programas exibe os aplicativos que você pode optar por excluir os registros de históricos.

- Selecione um ou mais nome de usuário e programa para excluir o histórico.
- Clique em **Excluir histórico agora** para confirmar.

Excluir histórico de forma manual ou automática

Você pode excluir os registros do histórico manualmente ou pode configurar o aplicativo para excluí-los automaticamente em intervalos especificados.

- **Manualmente**.
  Os registros de históricos somente serão excluídos ao clicar **Excluir histórico agora**.
- **A cada 10 minutos** ou **A cada hora**.
  Os registros de históricos serão automaticamente excluídos na frequência selecionada.
- Clique em **Salvar** para confirmar.

OBSERVAÇÃO: Se selecionar excluir o histórico Manualmente**, os registros somente serão limpos se você clicar em** Excluir histórico agora**. Os registros NÃO serão excluídos automaticamente.**

Copyright © 1990-2010 Norman ASA

Exclusão Segura

Com este aplicativo é possível executar a exclusão segura de arquivos específicos. O conteúdo dos arquivos são permanentemente apagados e não pode ser recuperado.

É possível iniciar um processo de exclusão segura de arquivos simplesmente clicando com o botão direito do mouse. Você será solicitado a confirmar a exclusão. O progresso de exclusão é exibido e um resumo aparece quando o processo de exclusão estiver completo. Essa é a forma segura de excluir arquivos:

- Selecione um ou mais arquivos que deseja excluir.
- Clique com o botão direito do mouse no arquivo ou arquivos.
- Selecione **Exclusão Segura Norman** a partir do menu suspenso.
- Clique em **OK** para confirmar.
- Clique em **OK** para selecionar o diálogo de resumo.

O conteúdo dos arquivos agora foi permanentemente apagado do computador.

OBSERVAÇÃO: Excluir um arquivo utilizando o método de exclusão segura leva muito mais tempo que a exclusão comum de arquivos. Isso porque cada parte do arquivo é sobrescrita múltiplas vezes para impedir que qualquer vestígio do conteúdo original seja recuperado.

Se o processo de exclusão for interrompido após iniciado, o arquivo ainda será destruído, mas não com a segurança esperada.

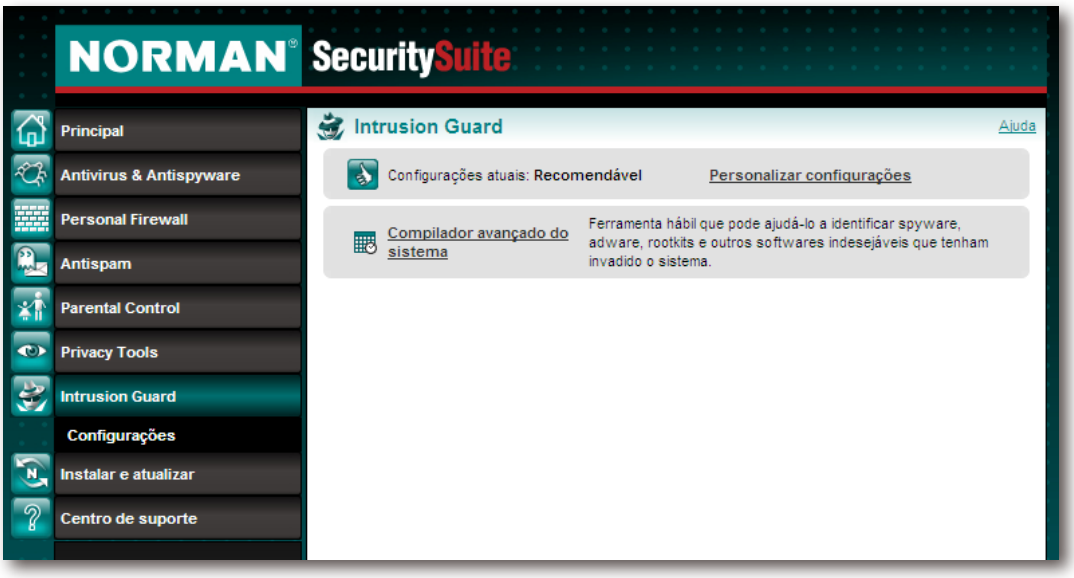
Alguns arquivos não podem ser excluídos. Isto acontece porque o usuário não tem permissão de gravar os arquivos ou porque o arquivo é protegido pelo sistema operacional e não pode ser excluído.

Copyright © 1990-2010 Norman ASA

Intrusion Guard

Abra o aplicativo Security Suite e selecione **Intrusion Guard** do menu do lado esquerdo. Consulte o “Guia de Introdução” na página 13 para obter instruções de como abrir o aplicativo e o “Intrusion Guard” na página 8 para obter uma descrição da finalidade e função do aplicativo.

Visualização principal



Este aplicativo é um sistema de prevenção de intrusos com base em host (HIPS) destinado a usuários experientes. Os usuários inexperientes devem manter as configurações recomendadas do produto, o que para a maioria dos casos é permitir e registrar eventos. Por padrão, somente são bloqueados eventos que têm um alto risco e são raramente utilizados por aplicativos legítimos.

Personalizar configurações

Clique nesta opção para editar os valores padrão. Consulte a seção “Configurações” na página 53. Para obter informações gerais sobre selecionar configurações recomendadas versus configurações personalizadas, consulte “Configurações do Security Suite” na página 15. Recomenda-se que apenas usuários avançados alterem as configurações padrão.

Relatório Avançado do Sistema

Essa é uma ferramenta destinada a usuários experientes. Com funcionalidade que possibilita detectar spyware e rootkits desconhecidos procurando anormalidades no computador. Consulte a seção “Apêndice B” na página 64.

Configurações

A partir desse diálogo é possível visualizar e editar a configuração do aplicativo. Na parte superior do painel de configuração selecione **Personalizar configurações** para utilizar suas próprias configurações personalizadas ou selecione **Configurações recomendadas** para retornar à configuração padrão.

OBSERVAÇÃO: Recomenda-se que apenas usuários avançados alterem as configurações padrão.

Copyright © 1990-2010 Norman ASA

Drivers e Memória

Intrusion Guard > Configurações
Ajuda
Configurações atuais: Recomendável
Personalizar configurações
Drivers e memória
Processos
Rede
Instalação do driver
Um driver do sistema pode acessar e controlar os dispositivos de hardware, para realizar isso, é concedido acesso total ao sistema, até mesmo aos aplicativos executados com privilégios de administrador. O que o Instrusion Guard deve fazer se um aplicativo tentar instalar drivers no sistema?
Prompt
Permitir
Negar
Acesso à memória física (apenas 32 bits)
Ao manipular a memória física diretamente, um aplicativo pode executar tarefas geralmente protegidas pelo sistema operacional. O que o Instrusion Guard deve fazer se um aplicativo tentar acessar a memória física?
Prompt
Permitir
Negar
Carregar e executar driver (apenas 32 bits)
Um aplicativo malicioso pode tentar carregar um driver do sistema sem instalá-lo primeiro. O que o Intrusion Guard deve fazer se um aplicativo tentar executar uma operação para carregar e executar drivers diretamente?
Salvar

Drivers são programas de computador que operam em uma nível baixo; o 'nível de kernel'. Os drivers são geralmente escritos para acessar e controlar hardwares, como monitor, teclado, impressora e placa de rede. Para acessar o hardware conectado ao computador, os drivers precisam de acesso total ao sistema. Por esse motivo as mesmas técnicas são utilizadas ao escrever aplicativos maliciosos. É possível modificar a configuração de instalação do driver para controlar quais aplicativos devem ter permissão para instalar drivers no computador.

Há duas técnicas maliciosas para obter os mesmos privilégios que os drivers obtêm. Ambas as técnicas burlam os mecanismos de segurança do sistema operacional. Recomenda-se enfaticamente manter as configurações para ambas as técnicas como **Negar**.

- **Solicitação**
  Você será solicitado a decidir todas as vezes que ocorrer uma tentativa.
- **Permitir**
  As tentativas apenas serão registradas.
- **Negar**
  Nenhum aplicativo, legítimo ou malicioso, poderá instalar drivers de nível de kernel.

Copyright © 1990-2010 Norman ASA

Processos

Intrusion Guard > Configurações
Ajuda
Configurações atuais: Recomendável
Personalizar configurações
Drivers e memória
Processos
Rede
Proteção de inicialização automática
Um aplicativo pode instruir o sistema operacional a inicializar-se automaticamente todas as vezes que a máquina iniciar ou um usuário efetuar login. O que o Intrusion Guard deve fazer quando um aplicativo tentar executar essa tarefa? (Observe que esse recurso não abrange o recurso AutoRun para CDs ou dispositivos USB).
Prompt
Permitir
Negar
Instalação de serviço
Um aplicativo pode instalar-se como um serviço em segundo plano, que faz com que ele seja executado todas as vezes que a máquina iniciar e também o executa com privilégios do sistema. O que o Intrusion Guard deve fazer quando um aplicativo tentar instalar um serviço?
Prompt
Permitir
Negar
Proteção de processos (apenas 32 bits)
O que o Intrusion Guard deve fazer se um aplicativo tentar usurpar outro processo injetando ameaças ou outro código nesse processo?
Permitir
Negar
Salvar

Quando um aplicativo, legítimo ou malicioso, é instalado no computador, ele na maioria dos casos desejará iniciar automaticamente sempre que o computador for ligado. Um programa que deseja iniciar automaticamente pode instruir o sistema operacional a inicializar-se automaticamente com os mesmos privilégios que o usuário atual ou pode instalar um serviço de fundo que será executado com privilégios elevados. O aplicativo de prevenção de intrusão pode interromper tentativas dessa natureza.

- **Solicitação**
  Você será solicitado a decidir todas as vezes que ocorrer uma tentativa.
- **Negar**
  Nenhum aplicativo, legítimo ou malicioso, poderá instalar-se para iniciar automaticamente quando o computador é ligado.

Um programa também pode injetar códigos em outros processos em execução na máquina e pode usurpar processos por outros meios. Esse é um comportamento comum para aplicativos maliciosos, mas alguns programas legítimos também utilizam tais técnicas, por exemplo, para estender a área de trabalho do usuário ou para oferecer outros recursos avançados ao sistema operacional ou aplicativos de terceiros. É possível configurar o aplicativo para recusar ou avisar a cada tentativa.

É possível editar uma lista de aplicativos confiáveis para incluir aplicativos legítimos com um comportamento semelhante.

Copyright © 1990-2010 Norman ASA

Rede

Intrusion Guard > Configurações
Ajuda
Configurações atuais: Recomendável
Personalizar configurações
Drivers e memória
Processos
Rede
Prevenção contra Plugins para IE
Os plugins para o Internet Explorer, como Objetos de ajuda de navegação e extensões de Barra de Ferramentas podem modificar e espionar dados enviados para seu navegador e a partir dele. O que o Intrusion Guard deve fazer se um aplicativo tentar instalar um plugin no Internet Explorer?
Prompt
Permitir
Negar
Prevenção LSP
Um Provedor de serviço em camadas (LSP) é um filtro de rede genérico que pode modificar e espionar dados enviados para todos os aplicativos na máquina e a partir deles. O que o Intrusion Guard deve fazer quando um aplicativo tentar instalar um LPS?
Prompt
Permitir
Negar
Proteção de arquivos hosts
Ao acessar um website, seu nome de domínio ("endereço web") é traduzido para um endereço IP antes que os dados sejam enviados para o servidor remoto e a partir dele. A máquina primeiramente procurará o nome do domínio nos arquivos HOSTS, o que significa que as entradas anularão qualquer endereço IP que o nome solucionaria. O que o Intrusion Guard deve fazer quando o arquivos HOSTS forem alterados?
Salvar

Ao adicionar filtros aos módulos de rede no sistema operacional, os aplicativos maliciosos podem roubar dados pessoais como números de seguro social, detalhes de cartão de crédito e senhas. O adware pode modificar dados de rede e enviar por meio desses filtros. Isso pode alterar os resultados nos mecanismo de pesquisa e exibir anúncios indesejáveis na área de trabalho e inseridos nas páginas da web visitadas.

Um BHO (Objeto Auxiliar do Navegador) é uma extensão para o Microsoft Internet Explorer. Esse e outros plug-ins do Internet Explorer, como as barras de ferramentas, têm pleno controle sobre o tráfego de rede para o Internet Explorer e a partir dele e podem interagir com a interface de usuário.

Um LSP (Provedor de Serviços em Camadas) é um filtro genérico na pilha de rede no Windows. Tem pleno controle sobre todo o tráfego de rede no computador.

Ao acessar um site pelo nome de domínio (endereço web) ele é traduzido para um endereço IP. Então os dados são enviados para um servidor remoto e a partir dele. O computador procurará primeiro o nome de domínio nos arquivos de hosts. Isso significa que as entradas ali anulam qualquer Endereço IP nas resoluções de nome. Aplicativos maliciosos podem alterar o arquivo de hosts e, assim, redirecionar o tráfego de rede para um site malicioso (o assim chamado “Pharming”).

- **Solicitação**
  Você será solicitado a decidir todas as vezes que ocorrer uma tentativa.
- **Negar**
  Impede todas as tentativas de modificar o sistema e arquivos de hosts e de instalar um BHO ou um LSP.

Copyright © 1990-2010 Norman ASA

Instalar e atualizar

Abra o aplicativo Security Suite e selecione **Instalar e Atualizar** do menu do lado esquerdo. Consulte o “Guia de Introdução” na página 13 sobre como abrir o aplicativo.

Visualização principal

O menu **Instalar e Atualizar** exibe, entre outras opções, uma lista de todo os produtos no Security Suite. A partir deste menu você pode adicionar ou remover produtos, iniciar atualizações, ativar o Assistente de Licença e alteração de idioma da instalação do Norman Security Suite.

OBSERVAÇÃO: Alterações nesta página podem exigir a reinicialização do sistema para que tenham efeito.

Personalizar configurações

Clique nesta opção para editar os valores padrão. Consulte a seção “Configurações” na página 58. Para obter informações gerais sobre selecionar configurações recomendadas versus configurações personalizadas, consulte “Configurações do Security Suite” na página 15.

Produtos licenciados

A lista de produtos licenciados exibe os produtos que estão instalados, seu status e quando a licença expirará. Nesta página, você pode adicionar ou remover produtos ou componentes na lista. Se você desmarcar um caixa de verificação, todo o produto correspondente será desinstalado. Se e quando novos produtos/componentes forem adicionados ao Norman Security Suite, eles serão baixados automaticamente. Todos os produtos selecionados são atualizados automaticamente por meio da Atualização via Internet do Norman Security Suite.

OBSERVAÇÃO: Se você desmarcar um caixa de seleção, os produtos não selecionados serão desinstalados.

Copyright © 1990-2010 Norman ASA

Atualizar todos os produtos

São fornecias atualizações frequentes para as definições de vírus e arquivos do programa. A atualização é feita via Internet ou rede interna. Após a atualização da Internet ter baixado um pacote, a atualização será automaticamente instalada. Após uma atualização, o programa poderá avisá-lo para reiniciar seu computador.

- Clique em **Atualizar todos os produtos** de uma vez para atualizar todo o Security Suite.

Ativar/desativar atualizações automáticas

Por padrão, as atualizações automáticas estão ativadas. Isso significa que as instalações do produto são atualizadas sempre que houver componentes ou arquivos de definição para serem atualizados. Para alterar as configurações de atualização automática, consulte a seção **Configurações> Selecionar o método de atualização**.

OBSERVAÇÃO: O software antivírus deve ser atualizado com frequência para descobrir e remover de forma eficaz malwares.

Selecionar o idioma do produto

É possível alterar o idioma selecionado durante a instalação. Selecione o idioma preferido no menu suspenso **Idioma do produto** e clique em **Salvar**. A alteração terá efeito após a próxima atualização.

Assistente de Licença

O Assistente de Licença verifica e atualiza a licença. Se você selecionar essa opção, um diálogo é exibido com informações sobre os produtos instalados e credenciais da chave de licença. Uma chave válida é necessária para atualizar a instalação.

Configurações

Selecionar o método de atualização

Esta opção permite escolher entre a atualização manual e automática. Recomendamos o método de atualização automática, pois é de extrema importância manter o software sempre atualizado.

Copyright © 1990-2010 Norman ASA

Atualizar manualmente

Selecione esta opção se você prefere iniciar manualmente a Atualização da Internet a partir da página principal Instalar e atualizar (Atualizar todos os produtos). É possível selecionar a Atualização da Internet do menu da bandeja do sistema.

OBSERVAÇÃO: A opção Atualizar manualmente exige um início forçado da função Atualização da Internet. Selecionar essa opção significa que o sistema NÃO será atualizado automaticamente. É altamente recomendável a atualização do software com frequência. Atualizar manualmente não é um método recomendado para uso diário, como executar a atualização pode ser facilmente esquecida.

Automaticamente em intervalos definidos

Selecione esta opção para que o programa se encarregue de efetuar automaticamente o download e a atualização. Selecione um intervalo de tempo na lista junto a **Automaticamente a cada** para definir o intervalo desejado. Essa opção requer uma conexão permanente com a Internet.

OBSERVAÇÃO: A opção Automaticamente em intervalos definidos significa que o sistema é atualizado automaticamente. Esse é o método de atualização recomendado. Se a Atualização via Internet não for realizada em 24 horas, o programa verifica automaticamente se há atualizações ao iniciar.

Aguardar a conexão dial-up

Se você usa um modem para se conectar à Internet, selecione esta opção para verificações diárias de atualizações nos servidores do produto. Basta acessar a Internet da forma normal e o programa irá verificar se arquivos de atualização estão disponíveis. Se você se conecta à Internet diversas vezes ao dia, o mecanismo de atualização somente verifica as atualizações em sua primeira conexão do dia. Por exemplo, se você se conecta à Internet uma vez por semana, o programa fará a verificação após estar conectado.

Configurações de proxy

Um servidor de proxy é um computador intermediário que reside entre o computador do usuário e a Internet. Ele pode ser utilizado para registrar o uso da Internet e bloquear o acesso a um website. O firewall no servidor de proxy também pode ser utilizado para bloquear o acesso à determinados websites ou páginas da web.

Se um firewall ou servidor proxy protege seu computador, você deve digitar as informações de proxy exigidas.

- Acesse **Instalar e Atualizar – Configurações – Configurações de proxy**
- Selecione **Utilizador servidor proxy** e digite um endereço de proxy e porta.
- Selecione **Efetuar login no servidor proxy** e digite nome de usuário, senha e domínio (para Desafios/Respostas do Windows NT), se aplicável.
  - A Autenticação de Desafios/Respostas do Windows é o formato usado para se conectar ao Windows 2000 Server ou Exchange.
  - A conta de usuário tem o seguinte formato: [*NT/2000domainname*]\[*accountname*]

Copyright © 1990-2010 Norman ASA

Centro de Suporte

Abra o aplicativo Security Suite e selecione **Centro de Suporte** do menu do lado esquerdo. Consulte o “Guia de Introdução” na página 13 sobre como abrir o aplicativo.

Visualização principal

O **Centro de Suporte** oferece informações sobre onde obter mais assistência que a documentação do produto e a ajuda on-line podem fornecer. Além de conter um função de reparo automático que pode ser útil se você experimentar problemas com o software instalado.

Ajuda e resolução de problemas

Clicar no link **Ajuda e resolução de problemas** o conduzirá ao website da Norman, que oferece diversos recursos úteis que, na maioria dos casos, ajudarão você. Nesse website, você encontrará:

- Suporte
- Centro de segurança
- **O Fórum de Suporte da Norman**

Se pesquisar esses recursos não resolver o problema, entre em contato com o fornecedor local ou com o Escritório Norman.

Informação de contato

Essa página fornece números de telefone e endereços para que você entre em contato com seu escritório/representante Norman. Essas informações também estão disponíveis na última página deste documento.

Copyright © 1990-2010 Norman ASA

Reparo automático

Se tiver algum problema com sua versão instalada do Security Suite, você sempre poderá tentar executar o reparo automático antes de contatar a equipe de suporte.

Ao clicar em **Reparo automático**, inicia-se um processo em segundo plano que verifica sua instalação e, se necessário, atualiza arquivos ou componentes. Você verá o símbolo de uma engrenagem no menu da bandeja quando o reparo automático estiver sendo executado. Consulte “Os ícones de aviso da bandeja” na página 14 para obter uma explicação sobre os ícones que afetam o Security Suite.

Se não tiver acesso à interface gráfica do usuário, você poderá executar `delnvc5.exe` em `c:\Arquivos de Programas\Norman\nvc\bin` e escolher a opção **Reparar**.

Visualizador de Registro de Mensagens

Este é um recurso que controla o aplicativo e exibe várias informações da mensagem incluindo o tipo, origem, data e hora, aplicativo e detalhes.

Copyright © 1990-2010 Norman ASA

Desinstalação do NSS

Para desinstalar o Norman Security Suite, dois métodos estão disponíveis. Um deles é utilizar o recurso de **Adicionar ou Remover programas** do Windows. O outro é utilizar o aplicativo de desinstalação do Norman.

1. A partir do sistema operacional Windows:
   - Selecione **Iniciar > Painel de Controle > Adicionar ou Remover programas**.
     - No Vista, selecione **Programas e Recursos**.
   - Role para localizar e selecionar o aplicativo Norman.
   - Selecione a opção **Remover**.
     - Quando o programa for removido, reinicie o computador.

2. Utilizando o aplicativo de desinstalação do Norman:
   - Selecione **Iniciar > Executar** e digite o local de `delnvc5.exe`
     - O local padrão é `C:\Arquivos de Programas\Norman\nvc\bin\delnvc5.exe`.
   - Selecione a opção **Remover**.
     - Quando solicitado, reinicie o computador.

Copyright © 1990-2010 Norman ASA

Apêndice A

O que é Sandbox?

Sandbox é o termo que melhor descreve a técnica utilizada para verificar se um arquivo está infectado por um vírus desconhecido. O nome não é escolhido aleatoriamente, pois o método permite que um possível código de vírus não confiável circule no computador – não no computador propriamente dito, mas em uma área simulada e restrita dentro dele. O Sandbox é equipado com tudo que um vírus espera encontrar em um computador de verdade. É um playground onde é seguro permitir que um vírus se reproduza, mas onde todas as etapas são cuidadosamente monitoradas e registradas. O vírus se expõe no Sandbox, e como suas ações são registradas, a cura para essa nova praga pode ser gerada automaticamente.

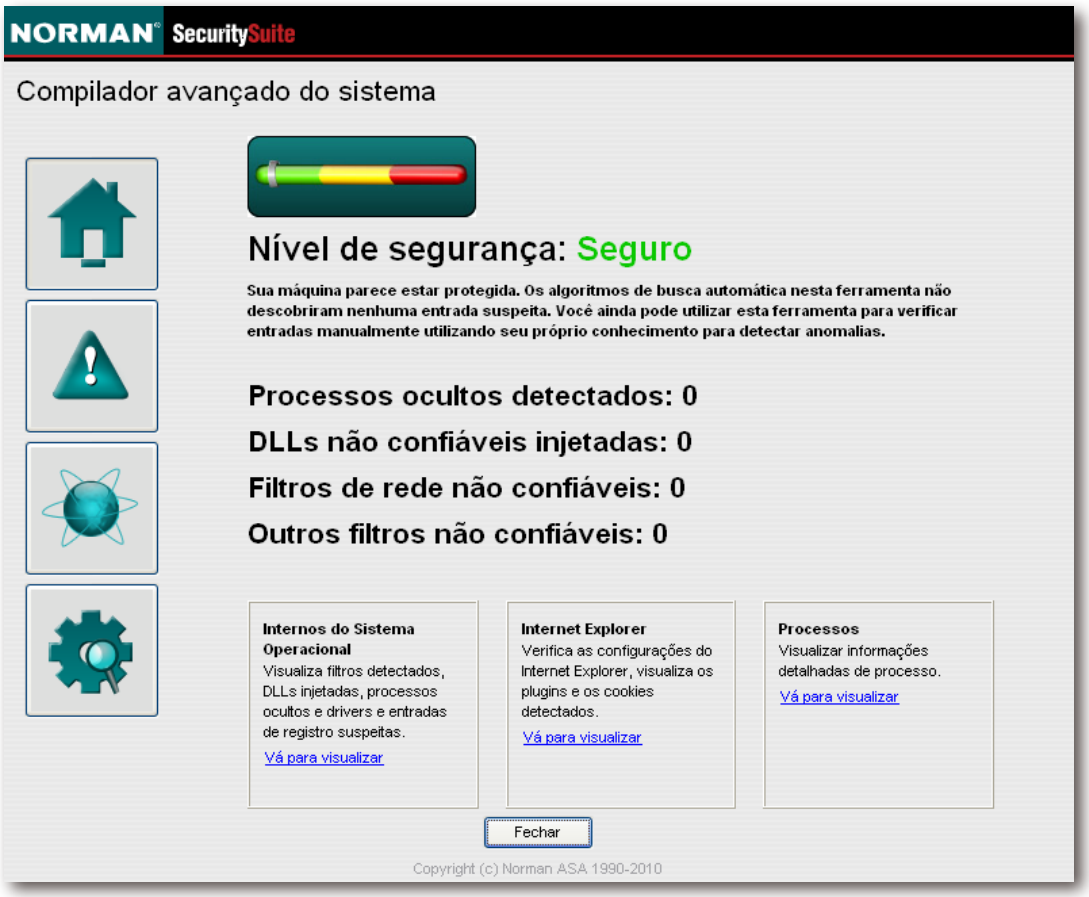
Hoje, um novo worm de e-mail pode infectar dezenas de milhares de estações de trabalho em questão de segundos. O recurso Sandbox da Norman pode ser uma ferramenta valiosa para capturar um novo código destrutivo.

Copyright © 1990-2010 Norman ASA

Apêndice B

Relatório Avançado do Sistema

Essa é uma ferramenta destinada a usuários experientes. Com funcionalidade que possibilita detectar spyware e rootkits desconhecidos procurando anormalidades no computador. Entradas suspeitas como processos ocultos, processos de inicialização automática desconhecidos, filtros de sistema desconhecidos etc. podem revelar aplicativos maliciosos.


NORMAN SecuritySuite
Compilador avançado do sistema
Nível de segurança: Seguro
Sua máquina parece estar protegida. Os algoritmos de busca automática nesta ferramenta não descobriram nenhuma entrada suspeita. Você ainda pode utilizar esta ferramenta para verificar entradas manualmente utilizando seu próprio conhecimento para detectar anomalias.
Processos ocultos detectados: 0
DLLs não confiáveis injetadas: 0
Filtros de rede não confiáveis: 0
Outros filtros não confiáveis: 0
Internos do Sistema Operacional
Visualiza filtros detectados, DLLs injetadas, processos ocultos e drivers e entradas de registro suspeitas.
Vá para visualizar
Internet Explorer
Verifica as configurações do Internet Explorer, visualiza os plugins e os cookies detectados.
Vá para visualizar
Processos
Visualizar informações detalhadas de processo.
Vá para visualizar
Fechar
Copyright (c) Norman ASA 1990-2010

Requisitos do Sistema Operacional

Visualizar e editar detalhes para processos ocultos e drivers, entradas de registro, filtros instalados e dlls injetadas.

Selecionar Internet Explorer

Visualizar e editar detalhes para configurações, plug-ins e cookies.

Processos

Visualizar e editar detalhes de processos para inicialização automática, serviços e outros processos.

Mesmo que o usuário experiente encontrará essas opções óbvias, ao clicar no link **O que é ...?** na área inferior da caixa de diálogo do Relatório Avançado do Sistema mais informações sobre vários assuntos serão fornecidas.

Copyright © 1990-2010 Norman ASA

Requisitos do Sistema Operacional

Processos Ocultos

Um processo oculto não é visível no modo de usuário, embora esteja atualmente em execução no computador. Um processo que é oculto do modo de usuário é oculto por um rootkit. Na maioria das vezes é um driver que oculta um processo malicioso do modo de usuário tornando-se invisível para o software antivírus padrão.

Se você descobrir processos ocultos no computador, é mais provável que um ou mais itens suspeitos estejam localizados sob a categoria de Filtros Instalados. Estas entradas são o rootkit em si.

Entradas de Registro

O registro interpreta de maneira diferente no modo de usuário e no modo kernel. Isso significa que algumas técnicas ocultam entradas do registro de aplicativos antivírus no modo de usuário. Qualquer entrada de registro que corresponda com essa técnica é considerada suspeita.

Filtros Instalados

Um filtro é um driver ou uma DLL que pode se conectar em um aplicativo, que pode alterar os dados antes que eles cheguem a um aplicativo.

- **LSP (Provedor de Serviços em Camadas)**
  Um LSP é um filtro de rede que é carregado para todos os aplicativos quando eles carregam o Win-Sock, que é o método mais comum para aplicativos de acesso à rede. Esses filtros de rede podem modificar e bloquear o tráfego de rede de entrada e saída do seu computador. Essa tecnologia é frequentemente utilizada por firewalls e filtros de de produtos de controle dos pais.
  Os filtros de rede maliciosos podem modificar os resultados da pesquisa, exibir anúncios indesejáveis e redirecioná-lo para sites maliciosos.
- **SSDT (System Service Dispatch Table)**
  Esse driver especial modifica o SSDT para operações realizadas por todos os aplicativos como abrir ou ler um arquivo ou iniciar uma nova aplicação. Essa técnica é comumente utilizada por empresas de segurança para impedir que aplicativos maliciosos façam alterações prejudiciais ao seus computadores.
  Entretanto, um driver SSDT malicioso pode ganhar capacidades poderosas de rootkit. Se você tiver um driver SSDT desconhecido na sua máquina e você ver um ou mais processos ocultos, isso indica uma alta probabilidade de um presença de rootkit.

DLLs injetadas

Uma DLL (Biblioteca de Vínculo Dinâmico) é um módulo do programa armazenado em um arquivo separado a fim de compartilhá-lo entre diferentes aplicativos ou para fornecer extensões para os aplicativos existentes. Uma DLL é carregada pelo aplicativo associado quando é necessário.

- **DLL injetada**
  É possível forçar um aplicativo a carregar uma DLL de terceiros. Isso é feito mesmo se o fornecedor do aplicativo não tiver projetado para isso acontecer e não carregar explicitamente a DLL. Essa técnica é amplamente utilizada para malware, porque o módulo de código dentro da DLL pode obter controle completo sobre o aplicativo. Ele também pode executar operações em nome do aplicativo, enganando o sistema operacional e o software de segurança para acreditar que o aplicativo executou a operação.
  Há alguns usos legítimos para injetar DLLs em outros aplicativos. Por exemplo, para depurar um aplicativo quando ele estiver danificado. De um modo geral, entretanto, um aplicativo que injeta DLLs em outros aplicativos ou é mal projetado ou é malicioso.
  Você deve tomar muito cuidado se encontrar DLLs injetadas em seu sistema. Qualquer DLL que não seja de um fornecedor completamente confiável deve ser removida. Mesmo o software que você tenha baixado e instalado a partir da Internet pode, na verdade, ser um trojan.

Drivers ocultos

Um driver oculto não é visível no modo de usuário, embora esteja em execução no computador. Um driver que está oculto no modo de usuário tem a funcionalidade ootkit. O driver oculta os arquivos no disco rígido, as entradas de registross ou o espaço de memória.

Copyright © 1990-2010 Norman ASA

Internet Explorer

Configurações
Visualizar e editar as configurações do Microsoft Internet Explorer.

Plug-ins
Um plug-in do navegador oferece recursos adicionais, como barras de ferramentas e acessórios de pesquisa, mas também pode oferecer anúncios indesejáveis e até mesmo espionar seus hábitos de navegação e senhas.

- **Objeto Auxiliar do Navegador**
  - Um Objeto Auxiliar do Navegador (BHO) é um plug-in do Internet Explorer que modifica o tráfego de entrada e saída do seu navegador. Esse tipo de plug-in é comumente utilizado por aplicativos spyware, porque facilmente capta todos os dados provenientes do navegador para o navegador.
- **Barra de ferramentas**
  - Uma barra de ferramentas é um plug-in do Internet Explorer que cria novas entradas no painel da barra de ferramentas do navegador. Aplicações adware utilizam esse tipo de plug-in para mostrar anúncios.
- **Motores de pesquisa de URL**
  - Os motores de pesquisa de URL redireciona endereços da web digitados e auxilia na resolução de endereços incorretos ou incompletos. Por exemplo, norman.com será traduzido, por padrão, para http://www.norman.com. Aplicativos adware utilizam esse tipo de plug-in para redirecioná-lo para outros websites.
- **Outros**
  - Outros plug-ins podem adicionar opções de menu ou painéis de usuário no navegador. Aplicações adware utilizam esse tipo de plug-in para mostrar anúncios.

OBSERVAÇÃO: Tecnicamente, todos os plug-ins são capazes de modificar o tráfego nos dados do usuário, mesmo quando o plug-in específico não tiver sido projetado para essa finalidade.

Cookies
Um cookie é um pequeno arquivo que é colocado na pasta de arquivos temporários da Internet quando você visita páginas da web.

- **Concepção errônea**
  - Um conceito errôneo comum sobre os cookies é que eles são mal-intencionados, geram pop-ups e anúncios indesejáveis e pode prejudicar o computador. De fato, alguns vendedores de antispyware relaciona os cookies como spyware e até mesmo geram alarmes sobre alguns cookies. Esse é especialmente o caso dos chamados "cookies de rastreamento".
  - Os cookies NÃO SÃO PERIGOSOS e não podem prejudicar o computador. Assim, os cookies exibidos nesta caixa de diálogo não constituem uma ameaça. Entretanto, se desejar, você poderá removê-los.
- **Utilização dos cookies**
  - Os servidores da web utilizam cookies para distinguir entre os usuários e para manter o estado. Se excluir um cookie, você perderá suas preferências, gráficos comerciais e o sistema de lembrar suas credenciais de login – mesmo com várias visitas. Será necessário, por exemplo, efetuar login novamente.
- **Cookies de rastreamento**
  - Alguns sites utilizam cookies de terceiros para controlar sua navegação no site. Alguns acham que isso é invasão de privacidade. Os servidores da web que você visitar também podem realizar a comunicação entre sites diretamente entre servidores e, portanto, não precisam confiar na ferramenta de rastreamento de cookies.
  - Nossa ferramenta não faz distinção entre cookies de rastreamento e cookies normais, uma vez que a única diferença é que o cookie de rastreamento é mantido por um terceiro. Não é mais nem menos perigoso do ponto de vista de malware.

Copyright © 1990-2010 Norman ASA

Processos

Inicialização automática

Quando um aplicativo, legítimo ou malicioso, é instalado no computador, ele na maioria dos casos desejará iniciar automaticamente sempre que o computador for ligado. Um programa que deseja iniciar automaticamente pode instruir o sistema operacional a inicializar-se automaticamente com os mesmos privilégios que o usuário atual ou pode instalar um serviço de fundo que será executado com privilégios elevados. O aplicativo de prevenção de intrusão pode interromper tentativas dessa natureza.

OBSERVAÇÃO: O recurso de inicialização automática não abrange o recurso de execução automática para CDs ou interfaces USB.

Serviços

Um serviço é um processo em segundo plano iniciado toda vez que o computador é iniciado. Esse é um comportamento normal.

Copyright © 1990-2010 Norman ASA

Escritórios da Norman

Danmark
Norman Data Defense Systems AS
Blangstedgårdsvej 1,
DK-5220 Odense SØ
Tel.: +45 63 11 05 08
Fax: +45 65 90 51 02
E-mail: info@normandk.com
Website: www.norman.com/dk

Deutschland
Norman Data Defense Systems GmbH
Zentrale, Gladbecker Str. 3,
D-40472 Düsseldorf
Tel.: +49 0211 5 86 99-0
Fax: +49 0211 5 86 99-150
E-mail: info@norman.de
Website: www.norman.com/de

España
Norman Data Defense Systems
Camino Cerro de los Gamos 1, Edif.1,
28224 Pozuelo de Alarcón MADRID
Tel.: +34 91 790 11 31
Fax: +34 91 790 11 12
E-mail: norman@normandata.es
Website: www.norman.com/es

France
Norman France
8 Rue de Berri,
F-75008 Paris
Tel.: +33 1 42 99 94 14
Fax: +33 1 42 99 95 01
E-mail: info@norman.fr
Website: www.norman.com/fr

Italia
Norman Data Defense Systems
Centro Cassina Plaza,
Via Roma, 108
20060 Cassina de'Pecchi (MI)
Tel.: +39 02 951 58 952
Fax: +39 02 951 38 270
E-mail: info@normanit.com
Website: www.norman.com/it

Nederland
Norman SHARK B.V.
Postbus 159,
2130 AD Hoofddorp
Tel.: +31 23 789 02 22
Fax: +31 23 561 31 65
E-mail: support@norman.nl
Website: www.norman.com/nl

Norge
Norman ASA
Matriz e vendas Noruega
Hovedkontor og salg Norge
Visite: Strandveien 37, Lysaker
Endereço para correspondência: PO Box 43, N-1324 Lysaker
Tel.: +47 67 10 97 00
Fax: +47 67 58 99 40
E-mail: norman@norman.no
Website: www.norman.com/no

Schweiz/Suisse/Svizzera
Norman Data Defense Systems AG
Münchensteinerstrasse 43
CH-4052 Basel
Tel.: +41 61 317 25 25
Fax: +41 61 317 25 26
E-mail: norman@norman.ch
Website: www.norman.com/ch

Sverige
Norman Data Defense Systems AB
Södra Grytsgatan 7, 2tr,
Norrköping Science Park
S-602 33 Norrköping
Tel.: +46 11 230 330
Fax: +46 11 230 349
E-mail: sales.se@norman.com
Website: www.norman.com/se

United Kingdom
Norman Data Defense Systems (UK) Ltd
Exchange House,
494 Midsummer Boulevard
Central Milton Keynes,
MK9 2EA
Tel.1: +44 08 707 448 044
Tel. 2: +44 01 908 255 990
Fax: +44 08 701 202 901
E-mail: info@normanuk.com
Website: www.norman.com/en-uk

United States
Norman Data Defense Systems Inc.
9302 Lee Highway,
Suite 950A,
Fairfax, Virginia 22031
Tel.: +1 703 267 6109
Fax: +1 703 934 6368
E-mail: norman@norman.com
Website: www.norman.com/en-us

A Norman ASA é uma das principais empresas na área de segurança de dados, proteção da internet e ferramentas de análise Por meio de sua tecnologia Sandbox a Norman oferece uma proteção exclusiva e proativa diferente de qualquer outro concorrente. Enquanto concentra-se em sua tecnologia antivírus proativa, a empresa fez alianças que permitem à Norman oferecer uma variedade completa de serviços de segurança de dados.

A Norman foi fundada em 1984 e é sediada na Noruega com a Europa Continental, Reino Unido e EUA como seus principais mercados.

NORMAN®

Copyright © 1990-2010 Norman ASA